(205,6,7)

1041-7
3-1

Journal für die reine und angewandte Mathematik

gegründet von A. L. Crelle 1826

fortgeführt von

C. W. Borchardt, K. Weierstrass, L. Kronecker,
L. Fuchs, K. Hensel, L. Schlesinger

gegenwärtig herausgegeben von

Helmut Hasse und Hans Rohrbach

unter Mitwirkung von

W. Brödel, M. Deuring, A. Grothendieck, P. R. Halmos, O. Haupt,
F. Hirzebruch, E. Hopf, M. Kneser, G. Köthe, K. Prachar,
P. Roquette, W. Schmeidler, L. Schmetterer, E. Stiefel

Band 205

In 4 Heften

Walter de Gruyter & Co.

vormals G. J. Göschen'sche Verlagshandlung / J. Guttentag, Verlagsbuchhandlung / Georg Reimer / Karl J. Trübner / Veit & Comp.

Berlin 1960/61

MATH
NMI
J8264
v. 205-207

March 30, 1962
B.P.

Archiv-Nr. 180360
Satz und Druck von Walter de Gruyter & Co., Berlin W 30
Printed in Germany

Inhaltsverzeichnis des Bandes 205

Seite

Benz, Walter, Über Winkel- und Transitivitätseigenschaften in Kreisebenen. I 48

Cigler, Johann, Der individuelle Ergodensatz in der Theorie der Gleichverteilung mod 1 91

Gilbert, Robert P., Singularities of Solutions to the Wave Equation in Three Dimensions 75

Golomb, Michael, On the Reducibility of Certain Linear Differential Systems 171

Härtter, Erich, Einige Abschätzungen für Abschnittsbasen 82

— —, Eine Verallgemeinerung des Basisbegriffes in der additiven Zahlentheorie 197

Hopf, Eberhard, On the Ergodic Theorem for Positive Linear Operators . . . 101

Klein-Barmen, Fritz, Über ein (max, min)-Theorem in der Theorie der Protoverbände und Dreigespanne 107

Meyer, C., Bemerkungen zu den allgemeinen Dedekindschen Summen 186

Oxtoby, John C., Spaces that admit a category measure 156

Plünnecke, Helmut, Über die Dichte der Summe zweier Mengen, deren eine die Dichte null hat 1

Rangachari, S. S., Modulare Korrespondenzen und L-Reihen 119

Schwarz, Wolfgang, Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen. I 21

Thomas, Johannes, Bemerkungen zu einem Satz von Pontrjagin und Tschebotarjow 113

Ausgabedaten der Hefte von Bd. 205

Heft 1/2 ausgegeben am 24. November 1960

Heft 3/4 ausgegeben am 30. Januar 1961

Über die Dichte der Summe zweier Mengen, deren eine die Dichte null hat.

Von *Helmut Plünnecke* in Hannover.

§ 1. Definitionen und Ergebnisse.

Bezeichnungen. Die Zeichen „$=_{\mathrm{Df}}$" und „$_{\mathrm{Df}}=$" sollen „Gleichheit per definitionem" bedeuten; dabei steht das definiens auf derselben Seite wie „$_{\mathrm{Df}}$".

$\rightarrow\ =_{\mathrm{Df}}$ Implikation; $\leftrightarrow\ =_{\mathrm{Df}}$ Äquivalenz; $\wedge\ =_{\mathrm{Df}}$ Konjunktion.

Lateinische und griechische Buchstaben $=_{\mathrm{Df}}$ reelle Zahlen.

Kleine lateinische Buchstaben $=_{\mathrm{Df}}$ ganze Zahlen.

$\mathfrak{g} =_{\mathrm{Df}}$ Menge der ganzen Zahlen.

Kleine deutsche Buchstaben $=_{\mathrm{Df}}$ Teilmengen von $\mathfrak{g}$.

Große deutsche Buchstaben $=_{\mathrm{Df}}$ Mengen nichtnegativer ganzer Zahlen.

$\mathfrak{Z} =_{\mathrm{Df}}$ Menge der natürlichen Zahlen.

$\mathring{\mathfrak{A}} =_{\mathrm{Df}} \mathfrak{A} \cup \{0\}$; $\emptyset =_{\mathrm{Df}}$ leere Menge.

$\{H(\xi, \eta) \mid \mathrm{Pr.}\,(\xi, \eta)\} =_{\mathrm{Df}}$ Menge aller ζ, die die Eigenschaft haben, daß es ξ, η so gibt, daß $H(\xi, \eta) = \zeta$ ist und daß die Aussage $\mathrm{Pr.}\,(\xi, \eta)$ wahr ist.

$\mathrm{card}\,\mathfrak{a} =_{\mathrm{Df}}$ Kardinalzahl von $\mathfrak{a}$.

$$|\mathfrak{a}| =_{\mathrm{Df}} \begin{cases} \operatorname*{Max}_{a,a' \in \mathfrak{a}} (a - a'), & \text{wenn } \mathfrak{a} \neq \emptyset; \\ 0, & \text{wenn } \mathfrak{a} = \emptyset. \end{cases}$$

$[\xi] =_{\mathrm{Df}}$ größte ganze Zahl g mit $g \leqq \xi$.

$\langle \xi \rangle =_{\mathrm{Df}}$ kleinste ganze Zahl g mit $g \geqq \xi$.

Leere Summe $=_{\mathrm{Df}} 0$; leeres Produkt $=_{\mathrm{Df}} 1$.

Definitionen. Es sei

$\mathfrak{A} + \mathfrak{B} =_{\mathrm{Df}} \{a + b \mid a \in \mathfrak{A} \wedge b \in \mathfrak{B}\}$.

$A(\xi) =_{\mathrm{Df}}$ Anzahl der $a \in \mathfrak{A}$ mit $1 \leqq a \leqq \xi$ $_{\mathrm{Df}}=$ Anzahlfunktion der Menge $\mathfrak{A}$.

(Wir bezeichnen die Anzahlfunktion einer — durch einen großen deutschen Buchstaben bezeichneten — Menge immer mit dem zugehörigen großen lateinischen Buchstaben; $(A + B)(\xi)$ sei die Anzahlfunktion von $\mathfrak{A} + \mathfrak{B}$ usw.)

$$\delta(\mathfrak{A}) =_{\mathrm{Df}} \operatorname*{fin}_{n=1,2,3,\ldots} \frac{A(n)}{n} \;_{\mathrm{Df}}= \text{ finite Dichte von } \mathfrak{A}.$$

$$\delta^*(\mathfrak{A}) =_{\mathrm{Df}} \lim_{n=1,2,3,\ldots} \frac{A(n)}{n} \;_{\mathrm{Df}}= \text{ asymptotische Dichte von } \mathfrak{A}.$$

Nach A. Chintschin [2] nennt man eine Menge $\mathfrak{B}$ eine wesentliche Komponente, wenn $\delta(\mathfrak{A} + \mathfrak{B}) > \delta(\mathfrak{A})$ für alle $\mathfrak{A}$ mit $0 < \delta(\mathfrak{A}) < 1$ gilt. In Anlehnung daran wollen

wir eine Menge $\mathfrak{B}$ eine *finite* bzw. *asymptotische außerordentliche Komponente* nennen, wenn für jede Mengenfolge $\mathfrak{A}_i$, für die $\delta(\mathfrak{A}_i) \to +0$ bzw. $\delta^*(\mathfrak{A}_i) \to +0$ strebt,

$$(1) \qquad \frac{\delta(\mathfrak{A}_i + \mathfrak{B})}{\delta(\mathfrak{A}_i)} \to \infty \quad \text{bzw.} \quad \frac{\delta^*(\mathfrak{A}_i + \mathfrak{B})}{\delta^*(\mathfrak{A}_i)} \to \infty$$

gilt.

$\delta^*(\mathfrak{B}) > 0$ ist eine hinreichende Bedingung dafür, daß $\mathring{\mathfrak{B}}$ eine finite bzw. $\mathfrak{B}$ eine asymptotische außerordentliche Komponente ist. Hierfür genügt es offenbar zu zeigen, daß $\delta(\mathfrak{A}_i + \mathring{\mathfrak{B}})$ bzw. $\delta^*(\mathfrak{A}_i + \mathfrak{B})$ gleichmäßig in i positiv nach unten beschränkt ist. Sei also $\delta^*(\mathfrak{B}) = \beta^* > 0$. Zu jedem $\varepsilon > 0$ gibt es ein $n(\varepsilon) \geqq 1$ so, daß $B(n) \geqq (\beta^* - \varepsilon)n$ für $n \geqq n(\varepsilon)$ ist. Wegen $\delta(\mathfrak{A}_i) > 0$ ist $1 \in \mathfrak{A}_i$. Sei $\varepsilon = \frac{\beta^*}{2}$; dann ist $(A_i + \mathring{B})(n) \geqq 1 \geqq \frac{n}{n(\varepsilon)}$ für $1 \leqq n \leqq n(\varepsilon)$ und $(A_i + \mathring{B})(n) \geqq 1 + B(n-1) \geqq 1 + \varepsilon(n-1) \geqq \varepsilon n$ für $n > n(\varepsilon)$. Also ist $\frac{(A_i + \mathring{B})(n)}{n} \geqq \operatorname{Min}\left(\frac{1}{n(\varepsilon)}, \varepsilon\right)_{\mathrm{Df}} = \mu > 0$ für $n \geqq 1$ und daher $\delta(\mathfrak{A}_i + \mathring{\mathfrak{B}}) \geqq \mu > 0$. Wegen $\delta^*(\mathfrak{A}_i) > 0$ gibt es ein $a_0 \in \mathfrak{A}_i$. Es folgt $(A_i + B)(n) \geqq B(n - a_0) \geqq (\beta^* - \varepsilon)(n - a_0)$ für $n \geqq a_0 + n(\varepsilon)$ und daher $\delta^*(\mathfrak{A}_i + \mathfrak{B}) \geqq \beta^* > 0$.

In der vorliegenden Arbeit werden für außerordentliche Komponenten Bedingungen hergeleitet, die von Mengen der asymptotischen Dichte *null* erfüllt werden; dabei werden wir untere Abschätzungen für das Wachstum der in (1) stehenden Quotienten erhalten.

Weitere Definitionen. Wenn $f(s)$ eine Funktion mit dem Argumentbereich $\mathfrak{a}$ ist, so sei

$$\mathfrak{B}_f =_{\mathrm{Df}} \{f(s) \mid s \in \mathfrak{a} \wedge f(s) \in \mathfrak{Z}\}.$$

Für beliebiges, aber festes $\mathfrak{A}$ setzen wir

$$\delta(\mathfrak{A})_{\mathrm{Df}} = \alpha, \quad \delta^*(\mathfrak{A})_{\mathrm{Df}} = \alpha^*, \quad \delta(\mathfrak{A} + \mathring{\mathfrak{B}}_f)_{\mathrm{Df}} = \gamma_f, \quad \delta^*(\mathfrak{A} + \mathfrak{B}_f)_{\mathrm{Df}} = \gamma_f^*.$$

Im folgenden sei *stets*

$$r =_{\mathrm{Df}} \langle \varrho \rangle.$$

(2) $f(s)$ heiße *ϱ-approximierbar* von S_0 an mit den Konstanten M, U, V [kurz: $f = \mathrm{Ap}(\varrho, S_0, M, U, V)$], wenn folgendes gilt:

$$(2\mathrm{A}) \qquad \varrho > 1, \; S_0 > 0, \; U > 0.$$

(2B) $f(s)$ ist eine für $s \geqq S_0$ erklärte Funktion[1]), deren Werte ganze Zahlen sind.

(2C) Es gibt eine Funktion $F(\sigma)$ mit den Eigenschaften:

(2Ca) $F(\sigma)$ ist für $\sigma \geqq S_0$ erklärt, und es ist

$$|f(s) - F(s)| \leqq M \text{ für } s \geqq S_0.$$

$$(2\mathrm{Cb}) \qquad U\sigma^\varrho \leqq F(\sigma) \leqq V\sigma^\varrho \text{ für } \sigma \geqq S_0.$$

(2Cc) $F(\sigma)$ ist r-mal differenzierbar, und die Ableitungen genügen für $1 \leqq i \leqq r$ den Ungleichungen

$$U\sigma^{\varrho - i} \leqq F^{(i)}(\sigma) \text{ für } \sigma \geqq S_0.$$

(Ein Beispiel für (2) ist: $\varrho > 1$, $S_0 = 1$, $f(s) = [s^\varrho]$, $F(\sigma) = \sigma^\varrho$, $M = 1$, $U = \varrho + 1 - r$, $V = 1$.)

---

[1]) Für den Argumentbereich $\mathfrak{a}$ der Funktion f gilt also $\mathfrak{g} \geqq \mathfrak{a} \geqq \mathfrak{g} \frown [S_0, \infty)$.

(3) Induktiv sei definiert:

$$\omega_2 =_{\mathrm{Df}} 2,\ \omega_3 =_{\mathrm{Df}} 5;\ \omega_{r+2} =_{\mathrm{Df}} 3\,\omega_{r+1} - \omega_r \text{ für } r \geqq 2.$$

$$\varphi_r =_{\mathrm{Df}} \begin{cases} 1 & \text{für } r = 2,\ r = 3; \\ (3r)^{-1} & \text{für } r \geqq 4. \end{cases} \tag{4}$$

Das Hauptresultat, das in dieser Arbeit gewonnen wird, läßt sich nun in folgendem Kriterium zusammenfassen.

(5) **Kriterium für außerordentliche Komponenten.**

Sei $f = \mathrm{Ap}\,(\varrho, S_0, M, U, V)$. *Dann ist* $\mathring{\mathfrak{B}}_f$ *eine finite und* $\mathfrak{B}_f$ *eine asymptotische außerordentliche Komponente; und wenn wir*

$$\tilde{S}_0 = \mathrm{Max}\,(S_0, 1),\ \tilde{M} = \mathrm{Max}\,(M, 1),\ \tilde{U} = \mathrm{Min}\,(U, 1),\ \tilde{V} = \mathrm{Max}\,(V, 1),$$

$$C_f = 10^{-6} \cdot 8^{-r} \cdot r^{-\frac{5}{3}} \tilde{M}^{-\frac{4}{3}} \tilde{U}^{\frac{4}{3}} \tilde{V}^{-\frac{5}{3}} \cdot \tilde{S}_0^{-\varrho},$$

$$C_f^* = 2 \cdot 10^{-6} \cdot r^{-\frac{5}{3}} \tilde{M}^{-\frac{4}{3}} \tilde{U}^{\frac{4}{3}} \tilde{V}^{-\frac{5}{3}}$$

setzen, so gilt:

$$\gamma_f \geqq C_f \cdot \alpha^{1-\varphi_r \omega_r^{-1}}, \tag{5A}$$

$$\gamma_f^* \geqq C_f^* \cdot \alpha_f^{*\,1-\omega_r^{-1}}. \tag{5B}$$

Die durch (3) *definierten* ω_r *genügen ferner für* $r \geqq 2$ *der Ungleichung*

$$\frac{64}{35}\left(\frac{3}{2} + \frac{1}{2}\sqrt{5}\right)^{r-2} \leqq \omega_r \leqq 2\left(\frac{3}{2} + \frac{1}{2}\sqrt{5}\right)^{r-2}. \tag{5C}$$

Im Falle $f(s) = qs^2$ mit $q \in \mathfrak{Z}$ liefern (5A) und (5B) für kleine Dichten Verschärfungen bereits in [4] mitgeteilter Abschätzungen[2]).

In § 2 werden zunächst vorbereitende Hilfssätze hergeleitet; § 3 bringt den Kern des Beweises in Form einer Induktion über r. In § 4 folgt schließlich der Beweis von (5). In § 5 werden Beispiele von approximierbaren Funktionen angegeben und wird die Güte der durch (5A) und (5B) gegebenen Abschätzungen diskutiert.

§ 2. Hilfssätze.

Wir definieren:

(6) Für beliebige, für $s, \sigma \geqq S_0$ erklärte Funktionen $f(s)$, $F(\sigma)$ sei für $p \geqq 0$ und $s, \sigma \geqq S_0$

$$\Delta_p f(s) =_{\mathrm{Df}} f(s+p) - f(s) \text{ und } \Delta_p F(\sigma) =_{\mathrm{Df}} F(\sigma + p) - F(\sigma).$$

(7) $f(s)$ heiße *ϱ-abschätzbar* von S_0 an mit den Konstanten M, U [kurz: $f = \mathrm{Ab}\,(\varrho, S_0, M, U)$], wenn folgendes gilt:

(7A) $\varrho > 0,\ S_0 \geqq 1,\ M \geqq 1,\ 0 < U \leqq 1.$

(7B) Wie (2B).

(7C) Es gibt eine Funktion $F(\sigma)$ mit den Eigenschaften (2Ca) und (2Cc).

---

[2]) Vgl. § 5, Beispiel 3.

Aus (6) folgt:

Wenn $F(\sigma)$ für $\sigma \geqq S_0$ i-mal differenzierbar und $p \geqq 0$ ist, so ist $\Delta_p F(\sigma)$ i-mal differenzierbar, und für $\sigma \geqq S_0$ gilt

$$\frac{d^i}{d\sigma^i} \Delta_p F(\sigma) = \Delta_p F^{(i)}(\sigma).$$

Hilfssatz 1. *Sei* $f = \mathrm{Ab}\,(\varrho, S_0, M, U)$, $\varrho > 1$ *und* $p \geqq 1$. *Dann gilt*

$$\Delta_p f = \mathrm{Ab}\,(\varrho - 1,\ S_0, 2M, \tfrac{1}{2}U).$$

(8) *Beweis.* $f(s)$ erfülle zusammen mit $F(\sigma)$ die Bedingungen (2B), (2Ca) und (2Cc). Dann folgt:

(8A) $$\varrho - 1 > 0,\ S_0 \geqq 1,\ 2M \geqq 1,\ 0 < \tfrac{1}{2}U \leqq 1.$$

(8B) $\Delta_p f(s)$ ist für $s \geqq S_0$ erklärt und hat als Werte ganze Zahlen.

(8Ca) $\Delta_p F(\sigma)$ ist für $\sigma \geqq S_0$ erklärt, und es ist für $s \geqq S_0$

$$|\Delta_p f(s) - \Delta_p F(s)| = |f(s+p) - F(s+p) - (f(s) - F(s))| \leqq 2M.$$

(8Cc) $\Delta_p F(\sigma)$ ist $\langle \varrho - 1 \rangle$-mal differenzierbar, und für $1 \leqq i \leqq \langle \varrho - 1 \rangle$ und $\sigma \geqq S_0$ gilt (mit $0 < \vartheta < 1$)

$$\frac{d^i}{d\sigma^i} \Delta_p F(\sigma) = \Delta_p F^{(i)}(\sigma) = F^{(i)}(\sigma + p) - F^{(i)}(\sigma) = p \cdot F^{(i+1)}(\sigma + \vartheta p)$$
$$\geqq \begin{cases} pU(\sigma + \vartheta p)^{\varrho - (i+1)} \geqq U\sigma^{(\varrho-1)-i} & \text{für } 1 \leqq i \leqq \langle \varrho - 1 \rangle - 1 = r - 2, \\ pU(\sigma + \vartheta p)^{\varrho - r} \geqq pU(\sigma + p)^{\varrho - r} = p^{1+\varrho-r}\, U\left(\dfrac{\sigma}{p} + 1\right)^{\varrho - r} \\ \qquad \geqq U(\sigma + 1)^{\varrho - r} \geqq U(2\sigma)^{\varrho - r} \geqq \tfrac{1}{2}U\sigma^{\varrho - r} & \text{für } i = \langle \varrho - 1 \rangle = r - 1. \end{cases}$$

Hilfssatz 2. *Sei* $f = \mathrm{Ab}\,(\varrho, S_0, M, U)$, $\varrho \geqq 1$, $p \geqq 0$, $0 < Q \leqq 1$, $QS \geqq S_0$ *und* $|\Delta_p f(s')| \leqq P$ *für mindestens ein* s' *mit* $QS \leqq s' \leqq S$. *Dann ist*

$$p \leqq U^{-1} Q^{1-\varrho} (2M + P)\, S^{1-\varrho}.$$

Beweis. Es gibt eine differenzierbare Funktion $F(\sigma)$ so, daß $|f(s) - F(s)| \leqq M$ und $U\sigma^{\varrho-1} \leqq F'(\sigma)$ ist für $s, \sigma \geqq S_0$. Es folgt (mit $0 < \vartheta < 1$)

$$|F(s' + p) - F(s')| \leqq |F(s' + p) - f(s' + p)| + |f(s' + p) - f(s')| + |f(s') - F(s')|$$
$$\leqq M + P + M = 2M + P,$$

$$2M + P \geqq |F(s' + p) - F(s')| \geqq F(s' + p) - F(s') = p \cdot F'(s' + \vartheta p)$$
$$\geqq pU(s' + \vartheta p)^{\varrho - 1} \geqq pUs'^{\varrho - 1} \geqq pUQ^{\varrho - 1} S^{\varrho - 1},$$
$$p \leqq U^{-1} Q^{1-\varrho} (2M + P)\, S^{1-\varrho}.$$

Hilfssatz 3. *Sei* $f = \mathrm{Ab}\,(\varrho, S_0, M, U)$, $\varrho \leqq 1$ *und* $S_0 \leqq S$. *Sei ferner* $f(s)$ *auf einer gewissen* q*-elementigen Teilmenge von* $[S_0, S] \cap \mathfrak{g}$ *konstant. Dann ist*

(9) $$q \leqq 3MU^{-1}S^{1-\varrho}.$$

Beweis. Da (9) für $q = 0$ trivial ist, sei im folgenden $q \geqq 1$ angenommen. Sei $f(s_1) = \cdots = f(s_q)$, $S_0 \leqq s_1$, $s_i + 1 \leqq s_{i+1}$ für $1 \leqq i \leqq q - 1$ und $s_q \leqq S$. Es folgt (ähnlich wie beim Beweise von Hilfssatz 2)

$$2M \geqq |F(s_q) - f(s_q) - (F(s_1) - f(s_1))| = |F(s_q) - F(s_1)| \geqq F(s_q) - F(s_1)$$
$$= (s_q - s_1) \cdot F'(s_1 + \vartheta(s_q - s_1)) \geqq (s_q - s_1)\, U(s_1 + \vartheta(s_q - s_1))^{\varrho - 1}$$
$$\geqq (s_q - s_1)\, U s_q^{\varrho - 1} \geqq (s_q - s_1)\, US^{\varrho - 1},$$
$$q \leqq s_q - s_1 + 1 \leqq 2MU^{-1}S^{1-\varrho} + 1 \leqq 3MU^{-1}S^{1-\varrho}.$$

Hilfssatz 4. *Sei* $j \geqq 1$, $\xi_i \geqq 0$ *für* $1 \leqq i \leqq j$, $0 < \tau \leqq 1$ *und* $\sum_{i=1}^{j} \xi_i \leqq j\xi$. *Dann ist*

$$\sum_{i=1}^{j} \xi_i^\tau \leqq j\xi^\tau.$$

Beweis. Da die Behauptung für $\tau = 1$ evident ist, sei im folgenden $0 < \tau < 1$ angenommen.

Die Funktion $\sum_{i=1}^{j} \eta_i^\tau$ besitzt auf der durch $\eta_i \geqq 0$ und $\sum_{i=1}^{j} \eta_i \leqq j\xi$ definierten, nichtleeren, abgeschlossenen Punktmenge (des j-dimensionalen Raumes) sicher ein Maximum, etwa bei $\eta_i = \mu_i$. Wäre $\mu_{i_1} \neq \mu_{i_2}$ für $1 \leqq i_1 < i_2 \leqq j$, so folgte $\mu_{i_1} + \mu_{i_2} \underset{\mathrm{Df}}{=} \mu > 0$;

$$\frac{d}{d\eta}\left(\eta^\tau + (\mu - \eta)^\tau\right) = \tau\left(\eta^{\tau-1} - (\mu - \eta)^{\tau-1}\right) \begin{cases} > 0 \text{ für } 0 < \eta < \frac{\mu}{2}, \\ = 0 \text{ für } \eta = \frac{\mu}{2}, \\ < 0 \text{ für } \frac{\mu}{2} < \eta < \mu; \end{cases}$$

$$\left(\frac{\mu}{2}\right)^\tau + \left(\frac{\mu}{2}\right)^\tau > \mu_{i_1}^\tau + \mu_{i_2}^\tau.$$

Setzen wir

$$\bar{\mu}_i = \begin{cases} \frac{\mu}{2} \text{ für } i = i_1 \text{ und } i = i_2, \\ \mu_i \text{ sonst,} \end{cases}$$

so erhalten wir den Widerspruch

$$\bar{\mu}_i \geqq 0, \sum_{i=1}^{j} \bar{\mu}_i = \sum_{i=1}^{j} \mu_i \leqq j\xi, \sum_{j=1}^{j} \bar{\mu}_i^\tau > \sum_{i=1}^{j} \mu_i^\tau.$$

Also ist $\mu_{i_1} = \mu_{i_2}$ für $1 \leqq i_1 \leqq i_2 \leqq j$. Da sicher $\sum_{i=1}^{j} \mu_i = j\xi$ ist, ist $\mu_i = \xi$ für $1 \leqq i \leqq j$ und daher

$$\sum_{i=1}^{j} \xi_i^\tau \leqq \sum_{i=1}^{j} \mu_i^\tau = j\xi^\tau.$$

§ 3. Induktion über r.

Wir definieren:

(10) Wenn $f(s)$ eine für $s \geqq S$ erklärte Funktion ist, deren Werte ganze Zahlen sind, und wenn mindestens eine der beiden Mengen $\mathfrak{e}_1$, $\mathfrak{e}_2$ endlich ist, so sei $\psi(\mathfrak{e}_1, \mathfrak{e}_2, S, T, f) \underset{\mathrm{Df}}{=}$ Anzahl der geordneten Tripel (e_1, e_2, s) mit $e_1 \in \mathfrak{e}_1$, $e_2 \in \mathfrak{e}_2$, $S \leqq s \leqq T$ und $e_1 = e_2 + f(s)$.

Im folgenden sei φ *stets* eine reelle Zahl mit

$$0 < \varphi \leqq 1;$$

φ_r erfüllt nach (4) für $r \geqq 2$ offenbar diese Bedingung.

(11) Ferner werde (induktiv) definiert:

$$\varkappa_1 =_{\mathrm{Df}} 2,\ \varkappa_{r+1} =_{\mathrm{Df}} \frac{2\varkappa_r + 1}{\varkappa_r + 1} \text{ für } r \geqq 1;$$

$$\lambda_1(\varphi) =_{\mathrm{Df}} 1 + \varphi,\ \lambda_{r+1}(\varphi) =_{\mathrm{Df}} \frac{\varkappa_r + \lambda_r(\varphi)}{\varkappa_r + 1} \text{ für } r \geqq 1;$$

$$\lambda_r =_{\mathrm{Df}} \lambda_r(1) \text{ für } r \geqq 1;$$

$$\bar{\lambda}_1(\varphi) =_{\mathrm{Df}} 1 + \varphi,\ \bar{\lambda}_{r+1}(\varphi) =_{\mathrm{Df}} 1 + \frac{1}{2}(\bar{\lambda}_r(\varphi) - \lambda_r(\varphi)) \text{ für } r \geqq 1.$$

(12) $$\zeta_r =_{\mathrm{Df}} \begin{cases} 0 \text{ für } r = 1, \\ 1 \text{ für } r \geqq 2. \end{cases}$$

Aus (11) folgt (induktiv):

(13) $1 < \varkappa_r \leqq 2,\ 1 < \lambda_r(\varphi) \leqq 2,\ 0 < \bar{\lambda}_r(\varphi) \leqq 2$ für $r \geqq 1$ und $\bar{\lambda}_r(\varphi) \leqq 1$ für $r \geqq 2$.

Hilfssatz 5. *Sei $f(s)$ eine für $s \geqq S$ erklärte Funktion, deren Werte ganze Zahlen sind, und $\mathfrak{e}$ eine endliche Menge. Dann gilt:*

I) $$\sum_{n \in \mathfrak{g}} \binom{\psi(\{n\}, \mathfrak{e}, S, T, f)}{2} = \sum_{p \geqq 1} \psi(\mathfrak{e}, \mathfrak{e}, S, T - p, \Delta_p f).$$

II) *Wenn $E = \operatorname{card} \mathfrak{e}$ und $j \geqq 1$ und $\mathfrak{e} = \bigcup_{i=1}^{j} \mathfrak{e}_i$ ist, so ist*

$$\psi(\mathfrak{e}, \mathfrak{e}, S, T, f) \leqq j\,E + 2 \sum_{i=1}^{j} \left(E \cdot \sum_{p \geqq 1} \psi(\mathfrak{e}_i, \mathfrak{e}_i, S, T - p, \Delta_p f)\right)^{\frac{1}{2}}.$$

Beweis. Ad I: Es ist

(14) $$\binom{\psi(\{n\}, \mathfrak{e}, S, T, f)}{2} = \text{Anzahl der geordneten Quadrupel } (e, e', s, s') \text{ mit } e, e' \in \mathfrak{e},\ S \leqq s < s' \leqq T \text{ und } n = e + f(s) = e' + f(s');$$

$$\psi(\mathfrak{e}, \mathfrak{e}, S, T - p, \Delta_p f) = \text{Anzahl der geordneten Tripel } (e, e', s) \text{ mit } e, e' \in \mathfrak{e},\ S \leqq s \leqq T - p \text{ und } e = e' + \Delta_p f(s).$$

Für $p \geqq 1$ folgt daher

$$S \leqq s \leqq T - p \longleftrightarrow S \leqq s < s + p \leqq T, \quad e = e' + \Delta_p f(s) \longleftrightarrow e + f(s) = e' + f(s+p),$$

(15) $$\psi(\mathfrak{e}, \mathfrak{e}, S, T - p, \Delta_p f) = \text{Anzahl der geordneten Quadrupel } (e, e', s, s+p) \text{ mit } e, e' \in \mathfrak{e},\ S \leqq s < s + p \leqq T \text{ und } e + f(s) = e' + f(s+p).$$

Aus (14) und (15) erhalten wir schließlich

$$\sum_{n \in \mathfrak{g}} \binom{\psi(\{n\}, \mathfrak{e}, S, T, f)}{2} = \{\text{Anzahl der geordneten Quadrupel } (e, e', s, s') \text{ mit } e, e' \in \mathfrak{e},\ S \leqq s < s' \leqq T \text{ und } e + f(s) = e' + f(s')\}$$
$$= \sum_{p \geqq 1} \psi(\mathfrak{e}, \mathfrak{e}, S, T - p, \Delta_p f).$$

Ad II: Für beliebige nichtnegative ganzzahlige r_i und $e \geqq 0$ gilt

$$r_i \geqq 2 \rightarrow r_i^2 \leqq r_i(2r_i - 2) = 4 \binom{r_i}{2},$$

$$\sum_{\substack{i=1 \\ r_i \geqq 2}}^{e} r_i \leqq \left(e \cdot \sum_{\substack{i=1 \\ r_i \geqq 2}}^{e} r_i^2\right)^{\frac{1}{2}} \quad \text{(nach der Cauchy-Schwarzschen Ungleichung),}$$

(16) $$\sum_{i=1}^{e} r_i \leqq \sum_{i=1}^{e} 1 + \sum_{\substack{i=1 \\ r_i \geqq 2}}^{e} r_i \leqq e + \left(e \cdot \sum_{i=1}^{e} 4 \binom{r_i}{2}\right)^{\frac{1}{2}} = e + 2\left(e \cdot \sum_{i=1}^{e} \binom{r_i}{2}\right)^{\frac{1}{2}}.$$

Aus (16) und Hilfssatz 5, I folgt schließlich

$$\psi(\mathfrak{e}, \mathfrak{e}, S, T, f) \leqq \sum_{i=1}^{j} \psi(\mathfrak{e}, \mathfrak{e}_i, S, T, f) = \sum_{i=1}^{j} \sum_{n \in \mathfrak{e}} \psi(\{n\}, \mathfrak{e}_i, S, T, f)$$
$$\leqq \sum_{i=1}^{j} \left(E + 2 \left(E \cdot \sum_{n \in \mathfrak{e}} \left(\frac{\psi(\{n\}, \mathfrak{e}_i, S, T, f)}{2} \right) \right)^{\frac{1}{2}} \right)$$
$$\leqq jE + 2 \sum_{i=1}^{j} (E \cdot \sum_{p \geqq 1} \psi(\mathfrak{e}_i, \mathfrak{e}_i, S, T - p, \Delta_p f))^{\frac{1}{2}}.$$

(17) **Hilfssatz 6.** *Es gelte*

(17A) $$f = \mathrm{Ab}\,(\varrho, S_0, M, U).$$

(17B) $$0 < Q \leqq 1, \; QS \geqq S_0, \; K \geqq 1.$$

(17C) $$|\mathfrak{e}| \leqq KS^{\varrho}, \; E = \mathrm{card}\,\mathfrak{e}, \; \varepsilon = E(KS^{\varrho} + 1)^{-1}.$$

(17D) $$C = 420\, MU^{-1}Q^{1-r}.$$

Dann ist

(17E) $$\psi(\mathfrak{e}, \mathfrak{e}, QS, S, f) \leqq C \cdot \varepsilon^{\lambda_r(\varphi)} \cdot K^{\varkappa_r} \cdot S^{\varrho+1} + \zeta_r \cdot 7 \cdot C \cdot \varepsilon^{\bar{\lambda}_r(\varphi)} \cdot K^{\varkappa_r} \cdot S^{\varrho+1-2^{2-r}}.$$

Beweis (durch vollständige Induktion nach r). Aus den Voraussetzungen folgt zunächst $r \geqq 1$, $S \geqq S_0 \geqq 1$, $M \geqq 1$, $0 < U \leqq 1$ und

(18) $$0 \leqq \varepsilon \leqq 1.$$

Induktionsanfang: $0 < \varrho \leqq 1$, also $r = 1$.

Sei χ die größte ganze Zahl q mit der Eigenschaft, daß es eine q-elementige Teilmenge von $[S_0, S] \cap \mathfrak{g}$ gibt, auf der $f(s)$ konstant ist. Nach (10) und Hilfssatz 3 folgt dann

$$\psi(\mathfrak{e}, \mathfrak{e}, S_0, S, f) \leqq \chi \cdot E^2 \leqq 3\, MU^{-1}S^{1-\varrho} \cdot E^2.$$

Nun ist $E^2 = \varepsilon^2(KS^{\varrho} + 1)^2 \leqq \varepsilon^2(2KS^{\varrho})^2 = 4\varepsilon^2K^2S^{2\varrho}$ und daher nach (13) und (11)

$$\psi(\mathfrak{e}, \mathfrak{e}, QS, S, f) \leqq \psi(\mathfrak{e}, \mathfrak{e}, S_0, S, f) \leqq 3\, MU^{-1}S^{1-\varrho} \cdot 4\varepsilon^2K^2S^{2\varrho}$$
$$\leqq C \cdot \varepsilon^{\lambda_1(\varphi)} \cdot K^{\varkappa_1} \cdot S^{\varrho+1},$$

woraus die Behauptung wegen (12) sofort folgt.

Induktionsschritt: $1 \leqq r$, $r - 1 < \varrho \leqq r$, $\varrho \to \varrho + 1$, also $r \to r + 1 = \langle \varrho + 1 \rangle$.

Wir setzen (17A) bis (17D) für $\varrho + 1$ statt ϱ voraus und nehmen Hilfssatz 6 für ϱ als bewiesen an.

Da (17E) für $\varepsilon = 0$ trivial ist, sei im folgenden $\varepsilon > 0$ angenommen. Dann ist $\mathfrak{e}$ nichtleer; e_0 sei das kleinste Element aus $\mathfrak{e}$. Sei L eine Konstante,

(19) $$L \geqq 1,$$

und für $i \geqq 1$

$$\mathfrak{e}_i = \mathfrak{e} \cap [e_0 + (i - 1)\, LS^{\varrho}, e_0 + iLS^{\varrho}),$$

(20) $$E_i = \mathrm{card}\,\mathfrak{e}_i \text{ und } \varepsilon_i = E_i(LS^{\varrho} + 1)^{-1}.$$

Dann ist für $i \geqq 1$

(21) $$|\mathfrak{e}_i| \leqq LS^{\varrho}.$$

Wenn (für $i \geqq 1$) $\mathfrak{e}_i \neq \emptyset$ ist, so folgt nach (17C) (für $\varrho + 1$ statt ϱ)

$$e_0 + (i - 1)\, LS^{\varrho} \leqq e_0 + |\mathfrak{e}| \leqq e_0 + KS^{\varrho+1},$$
$$i \leqq KL^{-1}S + 1.$$

Weiter erhalten wir[3])

$$(22)\qquad 1 \leqq j =_{\mathrm{Df}} [KL^{-1}S + 1] \leqq KL^{-1}S + 1 \;{}_{\mathrm{Df}}{=}\; J \leqq j + 1 \leqq 2J;$$

$$\mathfrak{e} = \mathop{\mathsf{U}^*}_{i=1}^{j} \mathfrak{e}_i, \quad \varepsilon_{j+1} = 0;$$

$$\varepsilon(KS^{\varrho+1} + 1) = E = \sum_{i=1}^{j} E_i = (LS^{\varrho} + 1) \sum_{i=1}^{j} \varepsilon_i,$$

$$\sum_{i=1}^{j+1} \varepsilon_i = \sum_{i=1}^{j} \varepsilon_i = \left(\frac{KS^{\varrho+1}}{LS^{\varrho} + 1} + \frac{1}{LS^{\varrho} + 1}\right) \varepsilon \leqq (KL^{-1}S + 1)\,\varepsilon = J\varepsilon \leqq (j + 1)\,\varepsilon,$$

also nach Hilfssatz 4 (mit $j + 1$ statt j) und (13)

$$(23)\qquad \sum_{i=1}^{j} \varepsilon_i^{\frac{1}{2}\lambda_r(\varphi)} \leqq 2J\varepsilon^{\frac{1}{2}\lambda_r(\varphi)}, \quad \sum_{i=1}^{j} \varepsilon_i^{\frac{1}{2}\bar{\lambda}_r(\varphi)} \leqq 2J\varepsilon^{\frac{1}{2}\bar{\lambda}_r(\varphi)}.$$

Wenn $i \geqq 1$, $p \geqq 1$ und $\psi(\mathfrak{e}_i, \mathfrak{e}_i, QS, S - p, \Delta_p f) \neq 0$ ist, so muß $|\Delta_p f(s')| \leqq |\mathfrak{e}_i| \leqq LS^{\varrho}$ für mindestens ein s' mit $QS \leqq s' \leqq S$ gelten; nach Hilfssatz 2 (mit $\varrho + 1$ statt ϱ und LS^{ϱ} statt P) folgt daher

$$(24)\qquad p \leqq U^{-1}Q^{-\varrho}(2M + LS^{\varrho})\,S^{-\varrho} \leqq U^{-1}Q^{-\varrho}(3MLS^{\varrho})\,S^{-\varrho} = DL,$$

wobei

$$(25)\qquad D =_{\mathrm{Df}} 3MU^{-1}Q^{-\varrho}$$

ist.

Für $p \geqq 1$ gilt nach Hilfssatz 1 (mit $\varrho + 1$ statt ϱ) $\Delta_p f = \mathrm{Ab}\,(\varrho, S_0, 2M, \frac{1}{2}U)$ und daher für $i \geqq 1$ (wegen (19), (21) und (20)) nach Induktionsvoraussetzung mit $\Delta_p f$ statt f, L statt K, $\mathfrak{e}_i$ statt $\mathfrak{e}$, E_i statt E, ε_i statt ε, $2M$ statt M, $\frac{1}{2}U$ statt U und

$$(26)\qquad C' =_{\mathrm{Df}} 1680\,MU^{-1}Q^{1-r}$$

statt C die Abschätzung

$$(27)\qquad \psi(\mathfrak{e}_i, \mathfrak{e}_i, QS, S - p, \Delta_p f) \leqq \psi(\mathfrak{e}_i, \mathfrak{e}_i, QS, S, \Delta_p f)$$
$$\leqq C' \cdot \varepsilon_i^{\lambda_r(\varphi)} \cdot L^{\varkappa_r} \cdot S^{\varrho+1} + \zeta_r \cdot 7 \cdot C' \cdot \varepsilon_i^{\bar{\lambda}_r(\varphi)} \cdot L^{\varkappa_r} \cdot S^{\varrho+1-2^{2-r}}.$$

Aus (24), (27) und (12) folgt

$$\sum_{p \geqq 1} \psi(\mathfrak{e}_i, \mathfrak{e}_i, QS, S - p, \Delta_p f)$$
$$\leqq DC' \cdot \varepsilon_i^{\lambda_r(\varphi)} \cdot L^{\varkappa_r+1} \cdot S^{\varrho+1} + 7DC' \cdot \varepsilon_i^{\bar{\lambda}_r(\varphi)} \cdot L^{\varkappa_r+1} \cdot S^{\varrho+1-2^{2-r}}.$$

Nach Hilfssatz 5, II und (23) ergibt sich daher

$$(28)\qquad \psi(\mathfrak{e}, \mathfrak{e}, QS, S, f) \leqq jE + 2\sum_{i=1}^{j}\left(E \cdot \sum_{p \geqq 1} \psi(\mathfrak{e}_i, \mathfrak{e}_i, QS, S - p, \Delta_p f)\right)^{\frac{1}{2}}$$
$$\leqq jE + 2\sum_{i=1}^{j} \{(DC' \cdot E \cdot \varepsilon_i^{\lambda_r(\varphi)} \cdot L^{\varkappa_r+1} \cdot S^{\varrho+1})^{\frac{1}{2}}$$
$$+ (7 \cdot DC' \cdot E \cdot \varepsilon_i^{\bar{\lambda}_r(\varphi)} \cdot L^{\varkappa_r+1} \cdot S^{\varrho+1-2^{2-r}})^{\frac{1}{2}}\}$$
$$\leqq JE + 4(DC')^{\frac{1}{2}} \cdot E^{\frac{1}{2}} \cdot J \cdot \varepsilon^{\frac{1}{2}\lambda_r(\varphi)} \cdot L^{\frac{1}{2}(\varkappa_r+1)} \cdot S^{\frac{1}{2}(\varrho+1)}$$
$$+ 3 \cdot 4\,(DC')^{\frac{1}{2}} \cdot E^{\frac{1}{2}} \cdot J \cdot \varepsilon^{\frac{1}{2}\bar{\lambda}_r(\varphi)} \cdot L^{\frac{1}{2}(\varkappa_r+1)} \cdot S^{\frac{1}{2}(\varrho+1)-2^{1-r}}.$$

---

[3]) „U^*" bedeutet „paarweise disjunkte Vereinigung".

Wir werden jetzt L in (28) geeignet wählen und haben dabei nur die Bedingung $L \geqq 1$ zu beachten. Nun ist nach (22) und (17C) (für $\varrho + 1$ statt ϱ)

$$J = KL^{-1}S + 1 \text{ und } E = \varepsilon(KS^{\varrho+1} + 1). \tag{29}$$

Daher ist (28) von der Form

$$\psi(\mathfrak{e}, \mathfrak{e}, QS, S, f) \leqq \{\varepsilon K^2 L^{-1} + \xi \cdot \varepsilon^{\frac{1}{2}(\lambda_r(\varphi)+1)} \cdot K^{\frac{3}{2}} \cdot L^{\frac{1}{2}(\varkappa_r - 1)}\} \cdot S^{\varrho+2} + o(S^{\varrho+2}) \tag{30}$$

(für $S \to \infty$), wobei ξ eine von ε, K, L und S unabhängige positive Konstante ist. Da von den beiden Summanden der geschweiften Klammer auf der rechten Seite von (30) der erste eine monoton fallende, der zweite eine monoton wachsende Funktion von L ist, liefert der durch Gleichsetzen der Summanden erhaltene Wert von L bis auf einen Faktor, der $\geqq \frac{1}{2}$ ist, die bestmögliche Abschätzung. Um $L \geqq 1$ zu gewährleisten, setzen wir

$$L = L_0 =_{\mathrm{Df}} \varepsilon^{-\frac{\lambda_r(\varphi)-1}{\varkappa_r+1}} K^{\frac{1}{\varkappa_r+1}}; \tag{31}$$

wegen (18), (13) und (17B) ist dann sicher $L = L_0 \geqq 1$. Wenn man $E \leqq 2\varepsilon KS^{\varrho+1}$ abschätzt, folgt nun aus (28)

$$\begin{aligned}\psi(\mathfrak{e}, \mathfrak{e}, QS, S, f) \leqq J \cdot \{&2\varepsilon K + 4(DC')^{\frac{1}{2}} \cdot \sqrt{2} \cdot \varepsilon K \\ &+ 3 \cdot 4(DC')^{\frac{1}{2}} \cdot \sqrt{2} \cdot \varepsilon^{1+\frac{1}{2}(\bar{\lambda}_r(\varphi) - \lambda_r(\varphi))} \cdot K \cdot S^{-2^{1-r}}\} \cdot S^{\varrho+1}.\end{aligned} \tag{32}$$

Nach (25), (26) und (17D) (für $\varrho + 1$ statt ϱ) ist

$$2 + 4(DC')^{\frac{1}{2}}\sqrt{2} = 2 + 4\sqrt{2}(3MU^{-1}Q^{-\varrho} \cdot 1680\, MU^{-1}Q^{1-r})^{\frac{1}{2}} \leqq C;$$

daher ergibt sich aus (32), (29), (31), (11), (13) und (12)

$$\begin{aligned}\psi(\mathfrak{e}, \mathfrak{e}, QS, S, f) &\leqq (KL_0^{-1}S + 1) \cdot C \cdot (\varepsilon \cdot K + 3 \cdot \varepsilon^{\bar{\lambda}_{r+1}(\varphi)} \cdot K \cdot S^{-2^{1-r}}) \cdot S^{\varrho+1} \\ &= C \cdot \Big\{\varepsilon^{1+\frac{\lambda_r(\varphi)-1}{\varkappa_r+1}} \cdot K^{2-\frac{1}{\varkappa_r+1}} \cdot S + \varepsilon \cdot K + 3 \cdot \varepsilon^{\bar{\lambda}_{r+1}(\varphi)+\frac{\lambda_r(\varphi)-1}{\varkappa_r+1}} \cdot K^{2-\frac{1}{\varkappa_r+1}} \cdot S^{1-2^{1-r}} \\ &\qquad + 3 \cdot \varepsilon^{\bar{\lambda}_{r+1}(\varphi)} \cdot K \cdot S^{-2^{1-r}}\Big\} \cdot S^{\varrho+1} \\ &\leqq C \cdot \{\varepsilon^{\lambda_{r+1}(\varphi)} \cdot K^{\varkappa_{r+1}} \\ &\qquad + (\varepsilon^{\bar{\lambda}_{r+1}(\varphi)} \cdot K^{\varkappa_{r+1}} + 3 \cdot \varepsilon^{\bar{\lambda}_{r+1}(\varphi)} \cdot K^{\varkappa_{r+1}} + 3 \cdot \varepsilon^{\bar{\lambda}_{r+1}(\varphi)} \cdot K^{\varkappa_{r+1}}) \cdot S^{-2^{1-r}}\} \cdot S^{\varrho+2} \\ &= C \cdot \varepsilon^{\lambda_{r+1}(\varphi)} \cdot K^{\varkappa_{r+1}} \cdot S^{\varrho+2} + \zeta_{r+1} \cdot 7 \cdot C \cdot \varepsilon^{\bar{\lambda}_{r+1}(\varphi)} \cdot K^{\varkappa_{r+1}} \cdot S^{\varrho+2-2^{2-(r+1)}}.\end{aligned}$$

§ 4. Beweis des Kriteriums (5).

Wir ziehen in Hilfssatz 7 zunächst einige Folgerungen aus den in (3), (4) und (11) gegebenen Definitionen.

Hilfssatz 7. *Es gilt:*

I) $\varphi\omega_r^{-1} = \dfrac{\lambda_{r-1}(\varphi) - 1}{\varkappa_{r-1}}$ *für* $r \geqq 2$;

II) $0 < \varphi\omega_r^{-1} < 1$ *für* $r \geqq 2$;

III) $(\varphi^{-1}\omega_r - 1)\,(\varrho - 1)^{-1} \geqq 1$ *für* $\varrho > 1$;

IV) $\varkappa_r \geqq \dfrac{3}{2}$ *für* $r \geqq 1$;

V) $\bar{\lambda}_{r-1}(\varphi_r) - \lambda_{r-1}(\varphi_r) + (\varphi_r\omega_r^{-1} - 1)\,(\varrho - 1)^{-1}(-2^{3-r}) \geqq 0$ *für* $\varrho > 1$.

Beweis. Offenbar ist

(33) $\varkappa_1 = 2, \quad \lambda_1(1) = \lambda_1 = 2, \quad \bar{\lambda}_1(1) = 2, \quad \omega_2 = 2, \quad \varphi_2 = 1,$

$\varkappa_2 = \frac{5}{3}, \quad \lambda_2(1) = \lambda_2 = \frac{4}{3}, \quad \bar{\lambda}_2(1) = 1, \quad \omega_3 = 5, \quad \varphi_3 = 1.$

(34) $\lambda_r(\varphi) - 1 = \varphi(\lambda_r - 1)$ für $r \geqq 1$. Induktionsbeweis klar.

(35) $\omega_r = \frac{\varkappa_{r-1}}{\lambda_{r-1} - 1}$ für $r \geqq 2$. Induktionsbeweis: Für $r = 2, r = 3$ richtig; weiter ist für $r \geqq 2$

$$\omega_{r+2} = 3\,\omega_{r+1} - \omega_r = 3\,\omega_{r+1} - \frac{\varkappa_{r-1}}{\lambda_{r-1} - 1} = 3\,\omega_{r+1} - \frac{\varkappa_{r-1}}{\varkappa_{r-1} + 1} \cdot \frac{\varkappa_{r-1} + 1}{\lambda_{r-1} - 1}$$
$$= 3\,\frac{\varkappa_r}{\lambda_r - 1} - \frac{\varkappa_r - 1}{\lambda_r - 1} = \frac{2\varkappa_r + 1}{\lambda_r - 1} = \frac{\varkappa_{r+1}(\varkappa_r + 1)}{\lambda_r - 1} = \frac{\varkappa_{r+1}}{\lambda_{r+1} - 1}.$$

Ad I: Die Richtigkeit folgt sofort aus (35), (34) und (13).

(36) $\omega_{r+1} \geqq \omega_r + 1 \geqq r + 1$ für $r \geqq 2$. (Insbesondere also $\omega_r \geqq r$ für $r \geqq 2$.) Induktionsbeweis klar.

Ad II *und* III: Die Behauptungen folgen aus $0 < \varphi \leqq 1$ und (36).

Ad IV: Induktionsbeweis klar.

(37) $\lambda_r - 1 \leqq \left(\frac{2}{5}\right)^{r-1}$ für $r \geqq 2$. Induktionsbeweis klar.

(38) $1 - \bar{\lambda}_r(\varphi) = \varphi \cdot \sum_{\nu=2}^{r-1} 2^{\nu-r}(\lambda_\nu - 1)$ für $r \geqq 2$. Induktionsbeweis (mittels (34)):

$1 - \bar{\lambda}_2(\varphi) = \frac{1}{2}\big(\lambda_1(\varphi) - \bar{\lambda}_1(\varphi)\big) = 0$; weiter ist für $r \geqq 2$

$$1 - \bar{\lambda}_{r+1}(\varphi) = \tfrac{1}{2}\,\big(\lambda_r(\varphi) - 1 + 1 - \bar{\lambda}_r(\varphi)\big)$$
$$= \frac{\varphi}{2}\,(\lambda_r - 1) + \varphi \cdot \sum_{\nu=2}^{r-1} 2^{\nu-r-1}(\lambda_\nu - 1) = \varphi \cdot \sum_{\nu=2}^{r} 2^{\nu-(r+1)}(\lambda_\nu - 1).$$

(39) $1 - \bar{\lambda}_r(\varphi) \leqq \varphi \cdot 2^{3-r}$ für $r \geqq 2$. Beweis (mittels (38) und (37)):

$$1 - \bar{\lambda}_r(\varphi) = \varphi \cdot \sum_{\nu=2}^{r-1} 2^{\nu-r}(\lambda_\nu - 1) \leqq \varphi \cdot \sum_{\nu=2}^{r-1} 2^{\nu-r}\left(\frac{2}{5}\right)^{\nu-1}$$
$$= \varphi \cdot 2^{1-r} \sum_{\nu=2}^{r-1} \left(\frac{4}{5}\right)^{\nu-1} \leqq \varphi \cdot 2^{1-r} \cdot \frac{\frac{4}{5}}{1 - \frac{4}{5}} = \varphi \cdot 2^{3-r}.$$

Ad V: Wegen $0 < \varphi_r \leqq 1$ und $\omega_r \geqq 1$ (nach (36)) ist für die Gültigkeit von Hilfssatz 7, V hinreichend

$$(1 - \varphi_r \omega_r^{-1})\,(r - 1)^{-1} \cdot 2^{3-r} \geqq \lambda_{r-1}(\varphi_r) - \bar{\lambda}_{r-1}(\varphi_r) \text{ für } r \geqq 2.$$

Für $r = 2$ und $r = 3$ folgt die letzte Ungleichung aus (33). Für $r \geqq 4$ erhalten wir nach (4), (37), (39) und (34)

(40)
$$(1 - \varphi_r \omega_r^{-1})\,(r - 1)^{-1} \cdot 2^{3-r} > \left(1 - \frac{1}{r}\right)(r - 1)^{-1} \cdot 2^{3-r}$$
$$= \varphi_r \cdot (1 + 2) \cdot 2^{3-r} = \varphi_r \cdot 2^{3-r} + \varphi_r \cdot 2^{4-r}$$
$$\geqq \varphi_r \cdot \left(\frac{2}{5}\right)^{r-2} + \varphi_r \cdot 2^{4-r} \geqq \varphi_r(\lambda_{r-1} - 1) + 1 - \bar{\lambda}_{r-1}(\varphi_r)$$
$$= \lambda_{r-1}(\varphi_r) - \bar{\lambda}_{r-1}(\varphi_r).$$

(41) **Hilfssatz 8.** *Es gelte:*

(41 A) $f = \mathrm{Ap}\,(\varrho, S_0, M, U, V)$.

(41 B) $S_1 \geqq S_0 \geqq 1,\ M \geqq 1,\ U \leqq 1,\ V \geqq 1$.

(41 C) $A(\xi) \geqq \alpha_0 \xi$ *für alle* ξ *mit* $\xi \geqq S_1^{\varrho-1}$, α_0 *eine positive Konstante.*

(41 D) $$T \geqq 8 \cdot \left(10^6 \cdot r M^{\frac{4}{3}} U^{-\frac{4}{3}} V^{\frac{2}{3}}\right)^{\frac{1}{\varrho-1}} \cdot V^{\frac{1}{\varrho}} \cdot S_1 \cdot \alpha_0^{(\varphi\omega_r^{-1}-1)(\varrho-1)^{-1}} \underset{\mathrm{Df}}{=} T_1(M, U, V, S_1, \alpha_0, \varphi)$$

(41 E) $\mathfrak{D} \geqq \mathfrak{B}_f$ *und* $(A + D)\,(T^\varrho) \geqq \alpha_0 T^\varrho$.

Dann gilt für die Anzahlfunktion der Menge $\mathfrak{A} + \mathfrak{D}$

(41 F) $$(A + D)\,(T^\varrho) \geqq 2 \cdot 10^{-6} \cdot r^{-\frac{5}{3}} M^{-\frac{4}{3}} U^{\frac{4}{3}} V^{-\frac{5}{3}} \cdot \alpha_0 \cdot \left(\alpha_0^{-\varphi\omega_r^{-1}} - \frac{1}{2} \cdot \alpha_0^{\bar{\lambda}_{r-1}(\varphi) - \lambda_{r-1}(\varphi) - \varphi\omega_r^{-1}} \cdot T^{-2^{3-r}}\right) \cdot T^\varrho.$$

Beweis. Statt der Voraussetzung (41 D) werde mit einer Konstanten K, von der wir

(42) $$K \geqq r \geqq 1$$

annehmen, zunächst allgemeiner vorausgesetzt:

(43) $$T \geqq 8 \cdot (M U^{-1} V)^{\frac{1}{\varrho}} \cdot S_1 \cdot K^{(\varphi^{-1}\omega_r - 1)(\varrho-1)^{-1}} \underset{\mathrm{Df}}{=} T_0(K).$$

Es ist

(44) $$S \underset{\mathrm{Df}}{=} 2^{-\frac{1}{\varrho}} V^{-\frac{1}{\varrho}} T \leqq T \text{ und } 1 \geqq Q \underset{\mathrm{Df}}{=} \frac{r-1}{r} \geqq \frac{1}{2}.$$

Aus (43), (44) und (42) folgt (nach Hilfssatz 7, III):

(45) $$T \geqq 6K,\ T^\varrho \geqq 6M \geqq 6;\ S \geqq QS \geqq 2S_1 K \geqq \begin{cases} S_1 \geqq S_0, \\ 2r, \end{cases} (QS)^\varrho \geqq 2MU^{-1};$$

(46) $$Q^{1-r} = \left(\frac{r}{r-1}\right)^{r-1} = \left(1 + \frac{1}{r-1}\right)^{r-1} \leqq 3,\ Q^{3-2r} = Q \cdot Q^{2\cdot(1-r)} \leqq 9.$$

Wegen (45) ist

(47) $$\bar{\mathfrak{B}} \underset{\mathrm{Df}}{=} \{f(s) \mid QS \leqq s \leqq S \wedge f(s) \in \mathfrak{Z}\} \leqq \mathfrak{B}_f \leqq \mathfrak{D}.$$

Wegen (41 C) läßt sich l (eindeutig) so bestimmen, daß

$$A(l) \geqq \alpha_0(KS^{\varrho-1} + 1) \text{ und } A(l-1) < \alpha_0(KS^{\varrho-1} + 1)$$

gilt; dann ist wegen (45) und (42)

(48) $$1 \leqq l \leqq KS^{\varrho-1} + 1.$$

Weiter ist

(49) $$\bar{\mathfrak{A}} \underset{\mathrm{Df}}{=} \mathfrak{A} \cap [1, l] \leqq \mathfrak{A},$$

(50) $$|\bar{\mathfrak{A}}| \leqq l - 1 \leqq KS^{\varrho-1},$$

(51) $$\operatorname{card} \bar{\mathfrak{A}} = A(l) \geqq \alpha_0(KS^{\varrho-1} + 1),$$

$$\begin{aligned} \operatorname{card} \bar{\mathfrak{A}} = A(l) &= A(l-1) + 1 \leqq (\alpha_0 + (KS^{\varrho-1} + 1)^{-1})\,(KS^{\varrho-1} + 1) \\ &\leqq (\alpha_0 + K^{-1} S^{1-\varrho})\,(KS^{\varrho-1} + 1) \end{aligned}$$

und daher

(52) $$\alpha_0 \leqq \operatorname{card} \bar{\mathfrak{A}} \cdot (KS^{\varrho-1} + 1)^{-1} \underset{\mathrm{Df}}{=} \alpha_1 \leqq \alpha_0 + K^{-1} S^{1-\varrho}.$$

Da (nach (49) und (47)) $\mathfrak{A} + \mathfrak{D} \geqq \bar{\mathfrak{A}} + \bar{\mathfrak{B}}$ ist, gilt

$$(53) \qquad (A + D)\,(T^\varrho) \geqq (\bar{A} + \bar{B})\,(T^\varrho).$$

Zum Beweise von (41 F) werden wir nun $(\bar{A} + \bar{B})\,(T^\varrho)$ in Abhängigkeit von K abschätzen und schließlich K geeignet wählen.

Da $f(s)$ approximierbar ist, gibt es eine Funktion $F(\sigma)$ so, daß für $s, \sigma \geqq S_0$

$$|\,f(s) - F(s)\,| \leqq M \text{ und } U\sigma^\varrho \leqq F(\sigma) \leqq V\sigma^\varrho$$

gilt. Für $QS \leqq s \leqq S$ folgt daher nach (45), (48) und (44)

$$(54) \quad f(s) \geqq F(s) - M \geqq Us^\varrho - M \geqq U(QS)^\varrho - M \geqq 2M - M = M \geqq 1,$$

$$(55) \quad l + f(s) \leqq l + F(s) + M \leqq KS^{\varrho-1} + 1 + Vs^\varrho + M$$
$$\leqq (KT^{-1} + T^{-\varrho} + VS^\varrho T^{-\varrho} + MT^{-\varrho})\,T^\varrho \leqq \left(\frac{1}{6} + \frac{1}{6} + \frac{1}{2} + \frac{1}{6}\right) T^\varrho = T^\varrho.$$

Wegen (47), (49) und (10) ist daher

$$\bar{\mathfrak{B}} = \{f(s) \mid QS \leqq s \leqq S\},$$

$$(56) \qquad n \in \bar{\mathfrak{A}} + \bar{\mathfrak{B}} \rightarrow 1 \leqq n \leqq T^\varrho,$$

$$(57) \qquad n \in \bar{\mathfrak{A}} + \bar{\mathfrak{B}} \longleftrightarrow \psi(\{n\}, \bar{\mathfrak{A}}, QS, S, f) \in \mathfrak{Z}.$$

Nun ist

$$x - \binom{x}{2} = x\left(1 - \frac{x-1}{2}\right) \begin{cases} = 0 \text{ für } x = 0, \\ \leqq 1 \text{ für } x \in \mathfrak{Z}. \end{cases}$$

Somit ergibt sich nach (56) und (57)

$$(58) \quad (\bar{A} + \bar{B})\,(T^\varrho) = \operatorname{card}(\bar{\mathfrak{A}} + \bar{\mathfrak{B}}) = \sum_{\substack{n \in \mathfrak{g} \\ \psi(\{n\}, \bar{\mathfrak{A}}, QS, S, f) \in \mathfrak{Z}}} 1$$
$$\geqq \sum_{n \in \mathfrak{g}} \psi(\{n\}, \bar{\mathfrak{A}}, QS, S, f) - \sum_{n \in \mathfrak{g}} \binom{\psi(\{n\}, \bar{\mathfrak{A}}, QS, S, f)}{2}.$$

Weiter gilt nach (44), (45) und (51)

$$(59) \quad \sum_{n \in \mathfrak{g}} \psi(\{n\}, \bar{\mathfrak{A}}, QS, S, f) = \psi(\mathfrak{g}, \bar{\mathfrak{A}}, QS, S, f) = \sum_{a \in \bar{\mathfrak{A}}} \psi(\mathfrak{g}, \{a\}, QS, S, f)$$
$$= \operatorname{card} \bar{\mathfrak{A}} \cdot ([S] - \langle QS \rangle + 1) \geqq \operatorname{card} \bar{\mathfrak{A}} \cdot (S - QS - 1)$$
$$= \operatorname{card} \bar{\mathfrak{A}} \cdot \left(\frac{1}{r} S - 1\right) \geqq S \cdot \operatorname{card} \bar{\mathfrak{A}} \cdot \left(\frac{1}{r} - \frac{1}{2r}\right)$$
$$\geqq S \cdot \alpha_0 (KS^{\varrho-1} + 1) \cdot \frac{1}{2r} \geqq \alpha_0 \cdot \frac{K}{4rV} \cdot T^\varrho.$$

Aus (41 A) und (41 B) folgt $f = \mathrm{Ab}\,(\varrho, S_0, M, U)$ und $\varrho > 1$ und für $p \geqq 1$ nach Hilfssatz 1

$$\Delta_p f = \mathrm{Ab}\,(\varrho - 1,\ S_0, 2M, \tfrac{1}{2}U).$$

Wegen (44), (45), (42), (50) und (52) sind daher für $p \geqq 1$ die Voraussetzungen des Hilfssatzes 6 mit $\Delta_p f$ statt f, $\varrho - 1$ statt ϱ, $2M$ statt M, $\frac{1}{2}U$ statt U, $\bar{\mathfrak{A}}$ statt $\mathfrak{e}$, card $\bar{\mathfrak{A}}$ statt E, α_1 statt ε und

$$(60) \qquad C_1 =_{\mathrm{Df}} 1680\, MU^{-1}Q^{2-r}$$

statt C erfüllt. Also gilt für $p \geqq 1$

$$(61) \quad \psi(\bar{\mathfrak{A}}, \bar{\mathfrak{A}}, QS, S - p, \Delta_p f) \leqq \psi(\bar{\mathfrak{A}}, \bar{\mathfrak{A}}, QS, S, \Delta_p f)$$
$$\leqq C_1 \cdot \alpha_1^{\lambda_{r-1}(\varphi)} \cdot K^{\varkappa_{r-1}} \cdot S^\varrho + \zeta_{r-1} \cdot 7 \cdot C_1 \cdot \alpha_1^{\bar{\lambda}_{r-1}(\varphi)} \cdot K^{\varkappa_{r-1}} \cdot S^{\varrho - 2^{3-r}}.$$

Wenn $p \geqq 1$ und $\psi(\bar{\mathfrak{A}}, \bar{\mathfrak{A}}, QS, S - p, \Delta_p f) \neq 0$ ist, dann muß $|\Delta_p f(s')| \leqq |\bar{\mathfrak{A}}| \leqq KS^{\varrho-1}$ für mindestens ein s' mit $QS \leqq s' \leqq S$ sein; nach Hilfssatz 2 (mit $KS^{\varrho-1}$ statt P) folgt

$$(62)\quad \begin{aligned} p &\leqq U^{-1}Q^{1-\varrho}(2M + KS^{\varrho-1})\, S^{1-\varrho} \\ &\leqq U^{-1}Q^{1-r}(3MKS^{\varrho-1})\, S^{1-\varrho} = 3MU^{-1}Q^{1-r} \cdot K. \end{aligned}$$

Nach Hilfssatz 5, I, (61), (62), (44) und (12) erhalten wir daher

$$(63)\quad \begin{aligned} &\sum_{n \in \mathfrak{G}} \binom{\psi(\{n\}, \bar{\mathfrak{A}}, QS, S, f)}{2} = \sum_{p \geqq 1} \psi(\bar{\mathfrak{A}}, \bar{\mathfrak{A}}, QS, S - p, \Delta_p f) \\ &\leqq 3MU^{-1}Q^{1-r} \cdot K \cdot (C_1 \cdot \alpha_1^{\lambda_{r-1}(\varphi)} \cdot K^{\varkappa_{r-1}} \cdot T^{\varrho} + 7 \cdot C_1 \cdot \alpha_1^{\bar{\lambda}_{r-1}(\varphi)} \cdot K^{\varkappa_{r-1}} \cdot T^{\varrho - 2^{3-r}}). \end{aligned}$$

Wegen (60) und (46) ist

$$(64)\quad \begin{aligned} C_2 &=_{\mathrm{Df}} 3MU^{-1}\, Q^{1-r} \cdot C_1 = 3MU^{-1}Q^{1-r} \cdot 1680\, MU^{-1}Q^{2-r} \\ &\leqq 27 \cdot 1680 \cdot M^2 U^{-2} \leqq 5 \cdot 10^4 \cdot M^2 U^{-2}. \end{aligned}$$

Aus (53), (58), (59), (63) und (64) ergibt sich schließlich

$$(65)\quad \begin{aligned} (A + D)\,(T^{\varrho}) \geqq \Big\{ &\alpha_0 \cdot \frac{K}{4rV} - C_2 \cdot \alpha_1^{\lambda_{r-1}(\varphi)} \cdot K^{\varkappa_{r-1}+1} \\ &- 7 \cdot C_2 \cdot \alpha_1^{\bar{\lambda}_{r-1}(\varphi)} \cdot K^{\varkappa_{r-1}+1} \cdot T^{-2^{3-r}} \Big\} \cdot T^{\varrho}. \end{aligned}$$

Wegen (41 E) gilt (65) auch ohne die Annahme (42) für jedes positive K. Aus $\xi_1 > 0$, $\xi_2 > 0$, $K > 0$ und

$$\frac{d}{dK}\left(\xi_1 \alpha_0 K - \xi_2 \alpha_0^{\lambda_{r-1}(\varphi)} K^{\varkappa_{r-1}+1}\right) = \xi_1 \alpha_0 - (\varkappa_{r-1} + 1)\, \xi_2 \alpha_0^{\lambda_{r-1}(\varphi)} K^{\varkappa_{r-1}} = 0$$

folgt nach (13) und Hilfssatz 7, I

$$K = (\xi_1(\varkappa_{r-1} + 1)^{-1} \xi_2^{-1})^{\frac{1}{\varkappa_{r-1}}} \cdot \alpha_0^{-\varphi\omega_r^{-1}}.$$

Wir wählen

$$K = K_0 =_{\mathrm{Df}} 10^{-5} \cdot r^{-\frac{2}{3}} M^{-\frac{4}{3}} U^{\frac{4}{3}} V^{-\frac{2}{3}} \cdot \alpha_0^{-\varphi\omega_r^{-1}}.$$

Dann lautet die Voraussetzung (43): $T \geqq T_9(K_0)$. Nach Hilfssatz 7, III und (41 D) ist

$$(66)\quad T_9(K_0) \leqq 8 \cdot (MU^{-1}V)^{\frac{1}{\varrho}} \cdot S_1 \cdot \alpha_0^{(\varphi\omega_r^{-1} - 1)(\varrho - 1)^{-1}} \leqq T_1(M, U, V, S_1, \alpha_0, \varphi).$$

Im folgenden wollen wir nun (41 D) voraussetzen; wegen (66) sind wir dann sicher, daß (65) mit $K = K_0$ gilt. Aus (52) und (44) folgt weiter

$$\begin{aligned} \alpha_1 &\leqq \alpha_0 + K_0^{-1} S^{1-\varrho} = \alpha_0 + K_0^{-1}(2V)^{\frac{\varrho-1}{\varrho}}\, T^{1-\varrho} \\ &\leqq \alpha_0 + 2V^{\frac{\varrho-1}{\varrho}} \cdot K_0^{-1} \cdot (T_1(M, U, V, S_1, \alpha_0, \varphi))^{1-\varrho} \\ &\leqq \alpha_0 + \frac{1}{5}\alpha_0 = \frac{6}{5}\alpha_0. \end{aligned}$$

Somit erhalten wir nach (64), (13) und Hilfssatz 7, IV, I

$$(67)\quad \begin{aligned} &\alpha_0 \cdot \frac{K_0}{4rV} - C_2 \alpha_1^{\lambda_{r-1}(\varphi)} K_0^{\varkappa_{r-1}+1} \\ &\geqq \alpha_0 \cdot \frac{1}{4} \cdot r^{-1} V^{-1} \cdot 10^{-5} \cdot r^{-\frac{2}{3}} M^{-\frac{4}{3}} U^{\frac{4}{3}} V^{-\frac{2}{3}} \cdot \alpha_0^{-\varphi\omega_r^{-1}} \\ &\quad - 5 \cdot 10^4 \cdot M^2 U^{-2} \cdot 2\alpha_0^{\lambda_{r-1}(\varphi)} \cdot 10^{-\frac{25}{2}} \cdot r^{-\frac{5}{3}} M^{-\frac{10}{3}} U^{\frac{10}{3}} V^{-\frac{5}{3}} \cdot \alpha_0^{1 - \lambda_{r-1}(\varphi) - \varphi\omega_r^{-1}} \\ &\geqq 2 \cdot 10^{-6} \cdot r^{-\frac{5}{3}} M^{-\frac{4}{3}} U^{\frac{4}{3}} V^{-\frac{5}{3}} \cdot \alpha_0^{1 - \varphi\omega_r^{-1}}, \end{aligned}$$

$$(68)\quad 7C_2 \cdot \alpha_1^{\bar{\lambda}_{r-1}(\varphi)} \cdot K_0^{\varkappa_{r-1}+1} \leqq 10^{-6} \cdot r^{-\frac{5}{3}} M^{-\frac{4}{3}} U^{\frac{4}{3}} V^{-\frac{5}{3}} \cdot \alpha_0^{1 + \bar{\lambda}_{r-1}(\varphi) - \lambda_{r-1}(\varphi) - \varphi\omega_r^{-1}}.$$

Durch Einsetzen von (67) und (68) in (65) folgt (41 F).

Beweis von (5A). Da (5A) für $\alpha = 0$ trivial ist, sei im folgenden $\alpha > 0$ vorausgesetzt. Aus den Voraussetzungen von (5A) folgt

$$(69) \qquad f = \mathrm{Ap}\,(\varrho, \tilde{S}_0, \tilde{M}, \tilde{U}, \tilde{V}),\ \tilde{S}_0 \geqq 1,\ \tilde{M} \geqq 1,\ \tilde{U} \leqq 1,\ \tilde{V} \geqq 1.$$

Nach Definition der Anzahlfunktion gilt für $\xi \geqq 1$

$$A(\xi) \geqq A([\xi]) \geqq \alpha[\xi] \geqq \frac{\alpha}{2}\,\xi$$

und, wegen $\mathfrak{A} + \mathring{\mathfrak{B}}_f \geqq \mathfrak{A}$,

$$(A + \mathring{B}_f)\,(\xi) \geqq A(\xi) \geqq \frac{\alpha}{2}\,\xi;$$

ferner ist nach (41D) und Hilfssatz 7, II

$$(70) \quad T_2(\varphi) =_{\mathrm{Df}} T_1(\tilde{M}, \tilde{U}, \tilde{V}, \tilde{S}_0, \frac{\alpha}{2}, \varphi) \geqq 1 \text{ und } \left(\frac{\alpha}{2}\right)^{1-\varphi\omega_r^{-1}} \geqq \frac{1}{2}\,\alpha^{1-\varphi\omega_r^{-1}}.$$

Also sind für $T \geqq T_2(\varphi)$ die Voraussetzungen des Hilfssatzes 8 mit $\tilde{S}_0$ statt S_0, $\tilde{M}$ statt M, $\tilde{U}$ statt U, $\tilde{V}$ statt V, $\tilde{S}_0$ statt S_1, $\frac{\alpha}{2}$ statt α_0 und $\mathring{\mathfrak{B}}_f$ statt $\mathfrak{D}$ erfüllt. Nach Hilfssatz 8 (für $\varphi = \varphi_r$) und Hilfssatz 7, V erhalten wir daher für $T \geqq T_2(\varphi_r)$

$$(71) \quad (A + \mathring{B}_f)\,(T^\varrho) \geqq 2 \cdot 10^{-6} \cdot r^{-\frac{5}{3}}\,\tilde{M}^{-\frac{4}{3}}\,\tilde{U}^{\frac{4}{3}}\,\tilde{V}^{-\frac{5}{3}} \cdot \frac{\alpha}{2} \cdot$$
$$\cdot \left(\left(\frac{\alpha}{2}\right)^{-\varphi_r\omega_r^{-1}} - \frac{1}{2}\left(\frac{\alpha}{2}\right)^{\bar{\lambda}_{r-1}(\varphi_r) - \lambda_{r-1}(\varphi_r) - \varphi_r\omega_r^{-1}} \cdot (T_2(\varphi_r))^{-2^{3-r}}\right) \cdot T^\varrho$$
$$\geqq \frac{1}{2} \cdot 10^{-6} \cdot r^{-\frac{5}{3}}\,\tilde{M}^{-\frac{4}{3}}\,\tilde{U}^{\frac{4}{3}}\,\tilde{V}^{-\frac{5}{3}} \cdot \alpha^{1-\varphi_r\omega_r^{-1}} \cdot T^\varrho.$$

(72) Wegen $\alpha > 0$ ist $1 \in \mathfrak{A}$.

Daher ist $1 \in \mathfrak{A} + \mathring{\mathfrak{B}}_f$ und für $1 \leqq T \leqq 8 \cdot \tilde{M}^{\frac{1}{\varrho}}\,\tilde{U}^{-\frac{1}{\varrho}}\,\tilde{V}^{\frac{1}{\varrho}} \cdot \tilde{S}_0$

$$(73) \qquad (A + \mathring{B}_f)\,(T^\varrho) \geqq 1 = T^\varrho \cdot T^{-\varrho} \geqq 8^{-\varrho} \cdot \tilde{M}^{-1}\,\tilde{U}\,\tilde{V}^{-1} \cdot \tilde{S}_0^{-\varrho} \cdot T^\varrho.$$

Sei schließlich $8 \cdot \tilde{M}^{\frac{1}{\varrho}}\,\tilde{U}^{-\frac{1}{\varrho}}\,\tilde{V}^{\frac{1}{\varrho}} \cdot \tilde{S}_0 \leqq T \leqq T_2(\varphi_r)$. Für $\frac{1}{4}\,\tilde{V}^{-\frac{1}{\varrho}} \cdot T \leqq s \leqq \frac{3}{4}\,\tilde{V}^{-\frac{1}{\varrho}} \cdot T$ folgt dann $s \geqq \tilde{S}_0$ und daher aus (69) (analog (54) bzw. (55))

$$(74) \quad f(s) \geqq \tilde{U}s^\varrho - \tilde{M} \geqq \tilde{U} \cdot 4^{-\varrho}\,\tilde{V}^{-1}\,T^\varrho - \tilde{M} \geqq 2^\varrho\,\tilde{M} - \tilde{M} \geqq \tilde{M} \geqq 1,$$

$$(75) \qquad 1 + f(s) \leqq 1 + \tilde{V}s^\varrho + \tilde{M} \leqq 1 + \left(\frac{3}{4}\right)^\varrho T^\varrho + \tilde{M}$$
$$\leqq \left(\frac{1}{8}\right)^\varrho T^\varrho + \left(\frac{3}{4}\right)^\varrho T^\varrho + \left(\frac{1}{8}\right)^\varrho T^\varrho \leqq T^\varrho.$$

Wegen (74) ist

$$\mathfrak{B}' =_{\mathrm{Df}} \left\{ f(s) \,\middle|\, \frac{1}{4}\,\tilde{V}^{-\frac{1}{\varrho}}\,T \leqq s \leqq \frac{3}{4}\,\tilde{V}^{-\frac{1}{\varrho}}\,T \right\} \subseteq \mathring{\mathfrak{B}}_f.$$

Nach (72), (75), (70) und (41D) gilt dann

$$(76) \quad (A + \mathring{B}_f)\,(T^\varrho) \geqq (A + B')\,(T^\varrho) \geqq \mathrm{card}\,\mathfrak{B}' \geqq \frac{1}{2}\,\tilde{V}^{-\frac{1}{\varrho}}\,T - 1 \geqq \frac{1}{4}\,\tilde{V}^{-\frac{1}{\varrho}}\,T$$
$$= \frac{1}{4}\,\tilde{V}^{-\frac{1}{\varrho}}\,T^{1-\varrho} \cdot T^\varrho \geqq \frac{1}{4}\,\tilde{V}^{-\frac{1}{\varrho}} \cdot (T_2(\varphi_r))^{1-\varrho} \cdot T^\varrho$$
$$\geqq 10^{-6} \cdot 8^{-r} \cdot r^{-1}\,\tilde{M}^{-\frac{4}{3}}\,\tilde{U}^{\frac{4}{3}}\,\tilde{V}^{-\frac{5}{3}} \cdot \tilde{S}_0^{1-\varrho} \cdot \alpha^{1-\varphi_r\omega_r^{-1}} \cdot T^\varrho.$$

Wegen Hilfssatz 7, II folgt aus (71), (73) und (76) für alle $T \geqq 1$

$$(77)\quad T^{-\varrho} \cdot (A + \mathring{B}_f)(T^\varrho) \geqq 10^{-6} \cdot 8^{-r} \cdot r^{-\frac{5}{3}} \widetilde{M}^{-\frac{4}{3}} \widetilde{U}^{\frac{4}{3}} \widetilde{V}^{-\frac{5}{3}} \cdot \widetilde{S}_0^{-\varrho} \cdot \alpha^{1-\varphi_r \omega_r^{-1}}.$$

Da

$$\gamma_f = \underset{n=\overline{1,2,3,\ldots}}{\underline{\mathrm{fin}}} \frac{(A + \mathring{B}_f)(n)}{n} \geqq \underset{T \geqq 1}{\underline{\mathrm{fin}}} \left(T^{-\varrho} \cdot (A + \mathring{B}_f)(T^\varrho)\right)$$

ist, erhalten wir aus (77) durch Übergang zum $\underline{\mathrm{fin}}$ die Ungleichung (5A).

Beweis von (5B). Da (5B) für $\alpha^* = 0$ trivial ist, sei im folgenden $\alpha^* > 0$ vorausgesetzt.

Aus den Voraussetzungen von (5B) folgt (69) und (analog (54)), daß $f(s) \geqq 1$ ist für alle hinreichend großen s. Also ist $\mathfrak{B}_f \neq \emptyset$; sei etwa $b_0 \in \mathfrak{B}_f$, dann ist $\mathfrak{A} + \mathfrak{B}_f \supseteqq \mathfrak{A} + \{b_0\}$. Nach Definition der Anzahlfunktion und der asymptotischen Dichte gilt nun für jedes ε mit $0 < \varepsilon < \alpha^*$ und bei festem ε für alle hinreichend großen ξ

$$A(\xi) \geqq A([\xi]) \geqq (\alpha^* - \varepsilon)[\xi] \geqq (\alpha^* - \varepsilon)(1 - \xi^{-1})\xi \geqq (\alpha^* - \varepsilon)(1 - \varepsilon)\xi;$$

$$\begin{aligned}(A + B_f)(\xi) &\geqq A(\xi - b_0) \geqq A([\xi - b_0]) \geqq (\alpha^* - \varepsilon)[\xi - b_0] \\ &\geqq (\alpha^* - \varepsilon)(1 - (b_0 + 1)\xi^{-1})\xi \geqq (\alpha^* - \varepsilon)(1 - \varepsilon)\xi.\end{aligned}$$

Also sind bei festem ε mit $0 < \varepsilon < \alpha^*$ die Voraussetzungen des Hilfssatzes 8 für alle hinreichend großen T mit $\widetilde{S}_0$ statt S_0, $\widetilde{M}$ statt M, $\widetilde{U}$ statt U, $\widetilde{V}$ statt V, S_1 hinreichend groß (aber fest), $(\alpha^* - \varepsilon)(1 - \varepsilon)$ statt α_0 und $\mathfrak{B}_f$ statt $\mathfrak{D}$ erfüllt. Folglich gilt dann für alle hinreichend großen T

$$(78)\quad T^{-\varrho} \cdot (A + B_f)(T^\varrho) \geqq 2 \cdot 10^{-6} \cdot r^{-\frac{5}{3}} \widetilde{M}^{-\frac{4}{3}} \widetilde{U}^{\frac{4}{3}} \widetilde{V}^{-\frac{5}{3}} \cdot \left((\alpha^* - \varepsilon)(1 - \varepsilon)\right)^{1-\varphi\omega_r^{-1}} - o(1)$$

(für $T \to \infty$). Da

$$\gamma_f^* = \underset{n=\overline{1,2,3,\ldots}}{\lim} \frac{(A + B_f)(n)}{n} \geqq \underset{T \to \infty}{\lim} \left(T^{-\varrho} \cdot (A + B_f)(T^\varrho)\right)$$

ist, erhält man aus (78) für $\varphi = 1$ durch Hintereinanderausführen der Grenzübergänge $T \to \infty$ und $\varepsilon \to 0$ die Ungleichung (5B).

Beweis von (5C). Wegen $\omega_r > 0$ (nach (36)) können wir $Q_r = \dfrac{\omega_{r+1}}{\omega_r}$ setzen.

Aus (3) folgt

$$\frac{\omega_{r+2}}{\omega_{r+1}} = 3 - \frac{\omega_r}{\omega_{r+1}},\ Q_{r+1} = 3 - Q_r^{-1},\ Q_2 = \frac{5}{2}.$$

Die Wurzeln der Gleichung $\xi^2 - 3\xi + 1 = 0$ sind

$$(79)\qquad \xi_1 = \frac{3}{2} + \frac{1}{2}\sqrt{5},\ \xi_2 = \frac{3}{2} - \frac{1}{2}\sqrt{5}.$$

$$(80)\qquad \frac{5}{2} \leqq Q_r < \xi_1.\ \text{Induktionsbeweis:}\ \frac{5}{2} = Q_2 < \xi_1;$$

Induktionsschritt $r \to r + 1$:

$$Q_r^{-1}(Q_r - \xi_2) = \frac{Q_r - \frac{3}{2} + \frac{1}{2}\sqrt{5}}{Q_r} = 1 - \frac{3 - \sqrt{5}}{2Q_r} \geqq 1 - \frac{3 - \sqrt{5}}{5} = \frac{2 + \sqrt{5}}{5}$$

$$\geqq \frac{4 + \frac{1}{6}}{5} = \frac{5}{6},$$

$$(81)\quad 0 < (\xi_1 - Q_r)\cdot\frac{5}{6} \leqq Q_r^{-1}(\xi_1 - Q_r)(Q_r - \xi_2) = Q_r^{-1}(3Q_r - Q_r^2 - 1)$$
$$= 3 - Q_r^{-1} - Q_r = Q_{r+1} - Q_r,$$
$$Q_{r+1} - Q_r = Q_r^{-1}(\xi_1 - Q_r)(Q_r - \xi_2) \leqq (\xi_1 - Q_r)\cdot\frac{2}{5}\cdot(\xi_1 - \xi_2) < \xi_1 - Q_r,$$
$$\frac{5}{2} \leqq Q_r < Q_{r+1} < \xi_1, \quad \text{q. e. d.}$$

Da die Gültigkeit von (80) für alle $r \geqq 2$ gezeigt wurde, gilt auch (81) allgemein. Es folgt

$$\xi_1 - Q_2 = \frac{\sqrt{5}-2}{2} \leqq \frac{1}{6},\ \xi_1 - Q_{r+1} = (\xi_1 - Q_r) - (Q_{r+1} - Q_r) \leqq (\xi_1 - Q_r)\cdot\frac{1}{6},$$
$$0 < \xi_1 - Q_r \leqq 6^{1-r}.$$

Weiter erhalten wir[4])

$$\left(1 - \frac{2}{5}\cdot 6^{-i}\right) = \left(1 + \frac{3}{7}\cdot 6^{-i}\right)^{-1}\cdot\left(1 + 6^{-i}\cdot\left(-\frac{2}{5} + \frac{3}{7} - \frac{6}{35}\cdot 6^{-i}\right)\right) \geqq \left(1 + \frac{3}{7}\cdot 6^{-i}\right)^{-1}$$

für $i \geqq 1$,

$$\prod_{i=1}^{r-1}\left(1 + \frac{3}{7}\cdot 6^{-i}\right) \leqq \prod_{i=1}^{r-1} e^{\frac{3}{7}\cdot 6^{-i}} \leqq e^{\frac{3}{7}\cdot\sum_{i=1}^{\infty} 6^{-i}} = e^{\frac{3}{7}\cdot\frac{1}{5}} = e^{\frac{3}{35}},$$

$$(82)\quad \prod_{i=2}^{r} Q_i = \prod_{i=2}^{r}(\xi_1 - (\xi_1 - Q_i)) \geqq \prod_{i=2}^{r}(\xi_1 - 6^{1-i}) = \xi_1^{r-1}\cdot\prod_{i=1}^{r-1}(1 - \xi_1^{-1}\cdot 6^{-i})$$
$$\geqq \xi_1^{r-1}\cdot\prod_{i=1}^{r-1}\left(1 - \frac{2}{5}\cdot 6^{-i}\right) \geqq \xi_1^{r-1}\cdot\prod_{i=1}^{r-1}\left(1 + \frac{3}{7}\cdot 6^{-i}\right)^{-1}$$
$$\geqq \xi_1^{r-1}\cdot e^{-\frac{3}{35}} \geqq \frac{32}{35}\cdot\xi_1^{r-1},$$

$$(83)\qquad \omega_2 = 2,\ \omega_{r+1} = \omega_2\cdot\frac{\omega_{r+1}}{\omega_2} = 2\cdot\prod_{i=2}^{r} Q_i \leqq 2\cdot\xi_1^{r-1}.$$

Aus (82), (83) und (79) schließen wir

$$\frac{64}{35}\left(\frac{3}{2} + \frac{1}{2}\sqrt{5}\right)^{r-1} \leqq \omega_{r+1} \leqq 2\cdot\left(\frac{3}{2} + \frac{1}{2}\sqrt{5}\right)^{r-1},$$

woraus sich wegen $\omega_2 = 2$ sofort (5C) ergibt.

Wegen $\varphi_r\omega_r^{-1} > 0$ bzw. $\omega_r^{-1} > 0$ folgt aus (5A) bzw. (5B) unmittelbar, daß $\mathfrak{B}_f$ eine finite bzw. $\mathfrak{B}_f$ eine asymptotische außerordentliche Komponente ist. Damit ist das Kriterium (5) vollständig bewiesen.

§ 5. Beispiele.

In diesem Paragraphen sollen nun zunächst Beispiele für approximierbare Funktionen angegeben werden.

Beispiel 1. *Sei*

$$j \geqq 0,\ \xi > 0,\ \varrho > 1,\ \varrho > \varrho_i \geqq 0 \text{ für } 1 \leqq i \leqq j,$$
$$\Theta = \sum_{i=1}^{j}|\xi_i|, \quad \tau = \operatorname*{Min}_{1\leqq i\leqq j}(\varrho - \varrho_i) \text{ für } j \geqq 1,$$
$$S_0 = \begin{cases} \operatorname{Max}\left(\left(\frac{2}{\xi}\cdot\frac{\Theta r}{\varrho + 1 - r}\right)^{\frac{1}{\tau j}}, 1\right), & \text{wenn } \Theta > 0 \text{ ist},\\ 1, & \text{wenn } \Theta = 0 \text{ ist},\end{cases}$$
$$F(\sigma) = \xi\sigma^{\varrho} + \sum_{i=1}^{j}\xi_i\sigma^{\varrho_i} \text{ für } \sigma > 0 \text{ und } f(s) = [F(s)] \text{ für } s > 0.$$

[4]) e bedeutet in den folgenden Formeln dieses Paragraphen die Basis der natürlichen Logarithmen.

Dann gilt

$$f = \mathrm{Ap}\left(\varrho, S_0, 1, \frac{\xi}{2}(\varrho + 1 - r), \frac{3}{2}\xi\right). \tag{84}$$

Beweis. Da (84) für $\Theta = 0$ sicherlich richtig ist, sei im folgenden $\Theta > 0$ angenommen. Für $s, \sigma \geqq S_0 \geqq 1$, $1 \leqq i \leqq j$ und $0 \leqq l \leqq r$ gilt dann:

$$|f(s) - F(s)| \leqq 1. \tag{85}$$

$$\begin{aligned} F(\sigma) &\leqq \xi\sigma^\varrho + \sum_{i=1} |\xi_i| \sigma^{\varrho_i} = \sigma^\varrho \left(\xi + \sum_{i=1}^{j} |\xi_i| \sigma^{-(\varrho-\varrho_i)}\right) \leqq \sigma^\varrho(\xi + \Theta\sigma^{-r}) \\ &\leqq \sigma^\varrho\left(\xi + \frac{\xi}{2}\right) = \frac{3}{2}\xi\sigma^\varrho. \end{aligned} \tag{86}$$

$$l - 1 \leqq \varrho_i \to \prod_{\nu=0}^{l-1} |\varrho_i - \nu| = \prod_{\nu=0}^{l-1} (\varrho_i - \nu) \leqq \prod_{\nu=0}^{l-1} (r - \nu);$$

$$\begin{aligned} \varrho_i \leqq l - 1 \to \prod_{\nu=0}^{l-1} |\varrho_i - \nu| &= \prod_{\nu=0}^{[\varrho_i]} (\varrho_i - \nu) \cdot \prod_{\nu=[\varrho_i]+1}^{l-1} (\nu - \varrho_i) \leqq \varrho_i \cdot \prod_{\nu=1}^{[\varrho_i]} ([\varrho_i] + 1 - \nu) \cdot \prod_{\nu=[\varrho_i]+1}^{l-1} \nu \\ &\leqq r \cdot \prod_{\nu=1}^{l-1} \nu \leqq \prod_{\nu=0}^{l-1} (r - \nu). \end{aligned}$$

$$\begin{aligned} \prod_{\nu=0}^{l-1} |\varrho_i - \nu| &\leqq \prod_{\nu=0}^{l-1} (r - \nu) = \prod_{\nu=0}^{l-1} \frac{r-\nu}{\varrho-\nu} \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu) \leqq \prod_{\nu=0}^{l-2} \frac{r-\nu}{\varrho-\nu} \cdot \frac{r-l+1}{\varrho-l+1} \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu) \\ &\leqq r \cdot \frac{1}{\varrho+1-r} \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu). \end{aligned}$$

$$\begin{aligned} \left|\frac{d^l}{d\sigma^l}\left(\sum_{i=1}^{j} \xi_i \sigma^{\varrho_i}\right)\right| &= \left|\sum_{i=1}^{j} \left(\xi_i \cdot \prod_{\nu=0}^{l-1} (\varrho_i - \nu) \cdot \sigma^{(\varrho-l)-(\varrho-\varrho_i)}\right)\right| \\ &\leqq \sigma^{\varrho-l} \cdot \sigma^{-r} \cdot \sum_{i=1}^{j} \left(|\xi_i| \cdot \prod_{\nu=0}^{l-1} |\varrho_i - \nu|\right) \\ &\leqq \sigma^{\varrho-l} \cdot \frac{\xi}{2} \cdot \frac{\varrho+1-r}{\Theta r} \cdot \sum_{i=1}^{j} |\xi_i| \cdot \frac{r}{\varrho+1-r} \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu) \\ &= \frac{\xi}{2} \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu) \cdot \sigma^{\varrho-l}. \end{aligned}$$

$$\begin{aligned} F^{(l)}(\sigma) &\geqq \xi \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu) \cdot \sigma^{\varrho-l} - \left|\frac{d^l}{d\sigma^l}\left(\sum_{i=1}^{j} \xi_i \sigma^{\varrho_i}\right)\right| \geqq \frac{\xi}{2} \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu) \cdot \sigma^{\varrho-l} \\ &\geqq \frac{\xi}{2} \cdot (\varrho + 1 - r) \cdot \sigma^{\varrho-l}. \end{aligned} \tag{87}$$

Aus (85), (86) und (87) folgt (84).

Beispiel 2[5]). *Sei*

$$q \in \mathfrak{Z},\ \varrho > 1,\ H \geqq \frac{2\varrho + 1}{\varrho + 1 - r},$$

$F(\sigma) = \sigma^\varrho \cdot (H + \sin \lg \sigma)$ *für* $\sigma > 0$ *und* $f(s) = q \cdot [F(s)]$ *für* $s > 0$.

Dann gilt

$$f = \mathrm{Ap}\,(\varrho, 1, q, 1, q \cdot (H + 1)). \tag{88}$$

---

[5]) Für $2 \geqq \varrho > 1$ und $H = \dfrac{2r+1}{\varrho+1-r} = \dfrac{5}{\varrho-1}$ liefert dieses Beispiel in Verbindung mit (5) Verschärfungen von bereits in [4], Fußnote 3, angegebenen Ungleichungen.

Beweis. Für $s, \sigma \geqq 1$ und $0 \leqq l \leqq r$ gilt:

$$(89) \qquad | f(s) - q \cdot F(s) | = q \cdot | [F(s)] - F(s) | \leqq q.$$

$$(90) \qquad q \cdot F(\sigma) \leqq q \cdot (H + | \sin\lg \sigma |) \cdot \sigma^{\varrho} \leqq q \cdot (H + 1) \cdot \sigma^{\varrho}.$$

$$\left.\begin{array}{l} A_0 = 1,\ A_{i+1} = (\varrho - i)\, A_i - B_i \text{ für } i \geqq 0, \\ B_0 = 0,\ B_{i+1} = (\varrho - i)\, B_i + A_i \text{ für } i \geqq 0, \end{array}\right\} \text{induktive Definition.}$$

$\dfrac{d^i}{d\sigma^i}(\sigma^{\varrho} \sin\lg \sigma) = \sigma^{\varrho - i}(A_i \sin\lg \sigma + B_i \cos\lg \sigma)$. Induktionsbeweis klar.

$| A_l | \leqq \varrho \cdot \prod\limits_{\nu=0}^{l-2} (\varrho - \nu)$, $| B_l | \leqq \varrho \cdot \prod\limits_{\nu=0}^{l-2} (\varrho - \nu)$. Induktionsbeweis: $l = 0$, $l = 1$ klar; für $1 \leqq l \leqq r - 1$ ist

$$\left.\begin{array}{l} | A_{l+1} | = | (\varrho - l)\, A_l - B_l | \leqq (\varrho - l)\, | A_l | + | B_l | \\ | B_{l+1} | = | (\varrho - l)\, B_l + A_l | \leqq (\varrho - l)\, | B_l | + | A_l | \end{array}\right\} \leqq (\varrho - l + 1) \cdot \varrho \cdot \prod_{\nu=0}^{l-2} (\varrho - \nu)$$
$$= \varrho \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu).$$

$$\left| \frac{d^l}{d\sigma^l} (\sigma^{\varrho} \sin\lg \sigma) \right| \leqq \sigma^{\varrho - l}(| A_l | + | B_l |) \leqq 2\varrho \prod_{\nu=0}^{l-2} (\varrho - \nu) \cdot \sigma^{\varrho - l}.$$

$$l \geqq 1 \rightarrow F^{(l)}(\sigma) \geqq H \cdot \prod_{\nu=0}^{l-1} (\varrho - \nu) \cdot \sigma^{\varrho - l} - \left| \frac{d^l}{d\sigma^l} (\sigma^{\varrho} \sin\lg \sigma) \right|$$
$$\geqq \left(\frac{2\varrho + 1}{\varrho + 1 - r} \cdot (\varrho + 1 - l) - 2\varrho \right) \cdot \prod_{\nu=0}^{l-2} (\varrho - \nu) \cdot \sigma^{\varrho - l} \geqq \prod_{\nu=0}^{l-2} (\varrho - \nu) \cdot \sigma^{\varrho - l}.$$

$F^{(l)}(\sigma) \geqq \sigma^{\varrho - l}$. (Gilt auch für $l = 0$.)

$$(91) \qquad \frac{d^l}{d\varrho^l} (q \cdot F(\sigma)) = q \cdot F^{(l)}(\sigma) \geqq \sigma^{\varrho - l}.$$

Aus (89), (90) und (91) folgt (88).

Beispiel 2 ist insofern bemerkenswert, als es uns für $q > 1$ finite bzw. asymptotische außerordentliche Komponenten $\mathring{\mathfrak{B}}_f$ bzw. $\mathfrak{B}_f$ liefert, die weder Basen[6]) noch wesentliche Komponenten[7]) sind und deren definierende Funktion f keine Abschätzung der Form $f(s) = \xi \cdot s^{\eta} + o(s^{\eta})$ (für $s \to \infty$ mit konstantem ξ, η und $\xi > 0$) gestattet.

Aus dem Beweis von Hilfssatz 7, V ist ersichtlich[8]), daß die in diesem Hilfssatz behauptete Ungleichung für $r \geqq 4$ auch noch für gewisse $\bar{\varphi}_r$ statt φ_r mit $\varphi_r < \bar{\varphi}_r \leqq 1$ erfüllt ist; man überzeugt sich an Hand des Beweises von (5A) sofort davon, daß dann auch (5A) mit $\bar{\varphi}_r$ statt φ_r gilt. Mir war es jedoch nicht möglich, (5A) für solche $\bar{\varphi}_r$ zu beweisen, für die nicht $r \cdot \bar{\varphi}_r = O(1)$ (für $r \to \infty$) gilt.

Was nun die in (5) auftretenden Konstanten C_f und C_f^* betrifft, so wurde lediglich darauf geachtet, daß diese Konstanten nicht gar zu ungünstig von r, $\tilde{M}$, $\tilde{U}$, $\tilde{V}$, $\tilde{S}_0$ abhängen. Daß sich die Abschätzungen (5A) und (5B) bezüglich der von α bzw. α^* unabhängigen konstanten Faktoren unter Umständen erheblich verbessern lassen, zeigt das folgende Beispiel.

---

[6]) Alle darstellbaren Elemente sind durch q teilbar.

[7]) Sei $\mathfrak{A} = \{1 + q\nu \mid \nu \in \mathring{\mathfrak{J}}\}$. Es folgt $0 < \delta(\mathfrak{A}) = \delta^*(\mathfrak{A}) = q^{-1} < 1$, $\mathfrak{A} = \mathfrak{A} + \mathring{\mathfrak{B}}_f \geqq \mathfrak{A} + \mathfrak{B}_f$.

[8]) In (40) steht das Größerzeichen.

Beispiel 3[9]. *Sei*

$$q \in \mathfrak{Z} \text{ und } f(s) = qs^2 \text{ für } s \geqq 1.$$

Dann ist

$$\gamma_f^* \geqq \frac{2}{3\sqrt{6q}}\,\alpha^{*\frac{1}{2}} - \alpha^*, \tag{92}$$

$$\gamma_f \geqq \frac{1}{7\sqrt{q}}\,\alpha^{\frac{1}{2}} - \alpha. \tag{93}$$

Beweisskizze. Wir erhalten die Ungleichungen (92) und (93), indem wir den in dieser Arbeit angegebenen Beweis für (5B) und (5A) für den Fall $f(s) = qs^2$ verfeinern. Der Einfachheit halber knüpfen wir an den Beweis des Hilfssatzes 1 aus [4] an[10].

Es gelte (2.1), (2.2), $0 \leqq \varepsilon < \bar{\alpha}$ und (2.3). Dann ist $2rkt_n \geqq m_\varepsilon$. Wir wählen l so, daß $A(l) \geqq (\bar{\alpha} - \varepsilon) \cdot 2rkt_n$ und $A(l-1) < (\bar{\alpha} - \varepsilon) \cdot 2rkt_n$ ist, und setzen $\mathfrak{A}' = \mathfrak{A} \cap [1, l]$. Es folgt $1 \leqq l \leqq 2rkt_n$, $A'(2rkt_n) = A(l) = A(l-1) + 1 \leqq \bar{\alpha} \cdot 2rkt_n + 1 = \bar{\alpha}(1 + (2rkt_n\bar{\alpha})^{-1})\,2rkt_n$ und $A'(m) \geqq (\bar{\alpha} - \varepsilon)\,m$ für $r(2ks_0 + k^2) \leqq m \leqq 2rkt_n$. Wenn wir jetzt die zum Beweise von Hilfssatz 1 aus [4] dienenden Abschätzungen mit $\mathfrak{A}'$ statt $\mathfrak{A}$ und $\varrho \geqq 1 + (2rkt_n\bar{\alpha})^{-1}$ durchführen und dabei beachten, daß $\sum_{s=s_0}^{t} L_s^{(m,k)} \leqq \binom{A'(2rkt_n)}{2}$ ist, so erhalten wir, ohne die Voraussetzung $0 \in \mathfrak{B}_r$ zu benutzen,

$$C_r(n) \geqq \bar{\alpha}n(k - 2\bar{\alpha}\varrho^2 rk^3) - \bar{\alpha}k(k + s_0)\sqrt{rn} - \varepsilon kn. \tag{94}$$

Hieraus folgen ähnlich wie in § 3 und § 4 von [4] die Ungleichungen (92) und (93).

Abschließend soll in (95) gezeigt werden, daß (93) bezüglich der Größenordnung in α für $\alpha \to 0$ nicht mehr allgemein verschärft werden kann. Wir formulieren diese Aussage mittels der Wirkungsfunktion, die wie folgt definiert ist[11]): (Finite) Wirkungsfunktion von $\mathfrak{B} =_{\mathrm{Df}} \operatorname{fin}_{\substack{\mathfrak{A} \\ \delta(\mathfrak{A}) \geqq \xi}} \delta(\mathfrak{A} + \mathfrak{B}) =_{\mathrm{Df}} \varphi(\xi, \mathfrak{B})$. Dies $\varphi(\xi, \mathfrak{B})$ ist bei festem $\mathfrak{B}$ offenbar eine monoton wachsende Funktion von ξ. Es gilt dann:

(95) *Falls $q \in \mathfrak{Z}$ und $f(s) = qs^2$ für $s \geqq 1$ ist, so ist für $0 < \xi \leqq 1$*

$$\frac{1}{7\sqrt{q}} \cdot \left(\frac{1}{\xi}\right)^{\frac{1}{2}} - 1 \leqq \frac{1}{\xi} \cdot \varphi(\xi, \mathring{\mathfrak{B}}_f) \leqq 4 + \frac{1}{\sqrt{q}} \cdot \left(\frac{1}{\xi}\right)^{\frac{1}{2}}.$$

Beweis. Die untere Abschätzung erhält man aus (93). Sei nun $\mathfrak{A}_m = \{1 + m\nu \mid \nu \in \mathring{\mathfrak{Z}}\}$ für $m \geqq 1$. Dann ist $\delta(\mathfrak{A}_m) = \dfrac{1}{m}$,

---

[9]) Offenbar gilt bestmöglich $f = \mathrm{Ap}(2, 1, 0, q, q)$. Daher liefern (5B) und (5A) mit $\tilde{S}_0 = \tilde{M} = \tilde{U} = 1$ und $\tilde{V} = q$ nur $\gamma_f^* \geqq 2 \cdot 10^{-6} \cdot 2^{-\frac{5}{3}} \cdot q^{-\frac{5}{3}} \cdot \alpha^{*\frac{1}{2}}$ und $\gamma_f \geqq 10^{-6} \cdot 8^{-2} \cdot 2^{-\frac{5}{3}} \cdot q^{-\frac{5}{3}} \cdot \alpha^{\frac{1}{2}}$.

[10]) Wir verwenden im folgenden *ausschließlich* die in [4] verwendeten Bezeichnungen; (2.—) bezieht sich auf die in [4] durchgeführte Numerierung.

[11]) Vgl. [3], I, S. 182.

$$\delta(\mathfrak{A}_m + \mathring{\mathfrak{B}}_f) \leqq \frac{(A_m + \mathring{B}_f)(m)}{m} = \frac{1}{m} + \frac{\mathring{B}_f(m-1)}{m} = \frac{1}{m} + \frac{1}{m} \cdot \left[\sqrt{\frac{m-1}{q}}\right] \leqq \frac{1}{m} + \frac{1}{\sqrt{qm}},$$

$$\xi \leqq \frac{1}{2} \to \varphi(\xi, \mathring{\mathfrak{B}}_f) \leqq \varphi([\xi^{-1}]^{-1}, \mathring{\mathfrak{B}}_f) \leqq \delta(\mathfrak{A}_{[\xi^{-1}]} + \mathring{\mathfrak{B}}_f) \leqq [\xi^{-1}]^{-1} + \frac{[\xi^{-1}]^{-\frac{1}{2}}}{\sqrt{q}}$$

$$\leqq 2\xi + \frac{1}{\sqrt{q}}\left(\xi^{\frac{1}{2}} + \frac{3}{2}\xi^{\frac{3}{2}}\right).$$

Da $\varphi(\xi, \mathring{\mathfrak{B}}_f) \leqq 1$ für $\xi \leqq 1$ ist, folgt hieraus die obere Abschätzung von (95).

Literaturverzeichnis.

[1] *A. Buchstab*, Über ein metrisches Problem der additiven Zahlentheorie. Mat. Sbornik **40** (1933), 190—195.

[2] *A. Khintchine* (*Čhintschin*), Über ein metrisches Problem der additiven Zahlentheorie. Mat. Sbornik **40** (1933), 180—189.

[3] *H. H. Ostmann*, Additive Zahlentheorie I, II. Ergebnisbericht, Springer-Verlag Berlin (1956).

[4] *H. Plünnecke*, Über ein metrisches Problem der additiven Zahlentheorie. Journ. reine angew. Math. **197** (1957), 97—103.

Eingegangen 27. Februar 1959.

Zur Darstellung von Zahlen durch Summen von Primzahlpotenzen[1].

I. Darstellung hinreichend großer Zahlen.

Von *Wolfgang Schwarz* in Erlangen.

Bezeichnungen und Vereinbarungen.

$\bigcup_i \mathfrak{M}_i$ mengentheoretische Vereinigung der Mengen $\mathfrak{M}_i$. Bei elementfremden Mengen schreiben wir auch $\sum_i \mathfrak{M}_i$.

$\varepsilon, \varepsilon', \ldots$ bedeutet stets eine beliebig kleine, fest vorgegebene positive Zahl.

$(x, \ldots, y)$ größter gemeinsamer Teiler der ganzen Zahlen $x, \ldots, y$.

$[\alpha]$ größte ganze Zahl $\leqq \alpha$.

$\| \alpha \|$ Abstand von α zur nächsten ganzen Zahl.

$f(z) \ll g(z)$ bedeutet dasselbe wie $f(z) = O(g(z))$.

$\exp(\alpha) = e^{\alpha}$, $e(\alpha) = e^{2\pi i \alpha}$.

$\pi(N; q, x)$ Anzahl der Primzahlen unterhalb N, die kongruent $x \bmod q$ sind.

$\pi(N) = \pi(N; 1, 0)$.

$p \mid q$: p ist Teiler von q; $p \nmid q$: p ist nicht Teiler von q.

$p^{\theta} \| q$: genau p^{θ} geht in q auf, also $p^{\theta} \mid q$, aber $p^{\theta+1} \nmid q$.

N, P, Q seien ganze, positive Zahlen, die stets als hinreichend groß vorausgesetzt werden.

$a, b_1, b_2, \ldots$ kleine lateinische Buchstaben außer $c, c_1, \ldots, e$ und z bedeuten stets ganze Zahlen.

Das Zahlenpaar a, q sei stets als teilerfremd vorausgesetzt, also $(a, q) = 1$.

$p, p', p_1, \ldots$ bedeuten stets Primzahlen.

$\alpha, \beta, \ldots, z$ sind reelle Veränderliche.

$c, c_1, c', \ldots$ bedeuten positive Konstanten. $c(\varepsilon, k)$ gibt an, wovon die Konstante abhängt.

$A < p_1, \ldots, p_s < B$ bedeute das Bestehen folgender s Ungleichungen: $A < p_\sigma < B$ $(\sigma = 1, \ldots, s)$.

$\left\{\sum_{x=1}^{r} + \sum_{x=s}^{t}\right\} f(x)$ bedeute $\sum_{x=1}^{r} f(x) + \sum_{x=s}^{t} f(x)$; analog ist $\left\{\int_A^B + \int_D^F\right\} g(\alpha)\, d\alpha$ zu verstehen.

Leere Produkte bedeuten 1, leere Summen 0.

---

[1]) Die Teile I und II dieser Arbeit sind eine überarbeitete Fassung meiner von der Naturwissenschaftlichen Fakultät der Universität Erlangen angenommenen Dissertation. Herrn Prof. Dr. Th. Schneider möchte ich für die Anregung dieser Arbeit und für wertvolle Ratschläge bei der Durchführung meinen herzlichsten Dank aussprechen.

Einleitung.

Durch die Verwendung von endlichen Exponentialsummen in seiner bahnbrechenden Arbeit (24) (vgl. Literaturverzeichnis)[2]) schaffte Vinogradov die Möglichkeit, additive Zerfällungen hinreichend großer ganzer Zahlen in Summen von Primzahlen und Primzahlpotenzen mit Hilfe der Hardy-Littlewoodschen Methode ohne Heranziehung irgendwelcher Hypothesen über die Nullstellenverteilung von Dirichletschen L-Funktionen zu untersuchen. Seither wurden Probleme dieser Art mehrfach bearbeitet.

Sei k eine feste, positive ganze Zahl, $f(x)$ ein Polynom vom Grade k mit ganzen Koeffizienten, den höchsten Koeffizienten als positiv vorausgesetzt; $p_1, p_2, \ldots$ mögen Primzahlen, $x_1, x_2, \ldots$ ganze Zahlen bedeuten. Dann wurden, wenn wir vom Waring-Problem für größere Exponenten absehen, hauptsächlich folgende additive Zerlegungen untersucht:

$N = p_1 + p_2 + p_3$ (Vinogradov (24)),

$N = a_1 p_1 + a_2 p_2 + a_3 p_3^k$, wobei die a_i ganze, teilerfremde Zahlen sind (v. d. Corput (1), mit $a_1 = a_2 = a_3 = 1$ auch Hua (12)).

$N = p_1 + p_2^2 + p_3^2 + p_4^k$ (Hua (12)).

$N = p_1 + x_1^2 + x_2^2 + x_3^k$ (Halberstam (9)).

$N = p_1^3 + \cdots + p_7^3 + x^3$ (Roth (22)).

$N = p_1 + p_2 + x^k$, $N = p_1 + \cdots + p_s + x_1^2 + \cdots + x_r^2$, wobei $2s + r > 4$ (Halberstam (9)).

$N = a_1 p_1 + \cdots + a_s p_s$, wobei $a_1, \ldots, a_s$ ganze, paarweise teilerfremde Zahlen sind (Richert (19)).

$N = p_1 + p_2^2 + p_3^3 + p_4^4 + p_5^5$ (Prachar (17)).

Wir wollen die Darstellbarkeit von N in der Gestalt

$$N = b_1 p_1 + \cdots + b_s p_s + f_1(p_1') + \cdots + f_r(p_r')$$

unter den Voraussetzungen $s \geqq 2$ und $r > 0$ oder $s > 2$ und $r \geqq 0$ untersuchen und eine asymptotische Formel für die Lösungsanzahl berechnen, um damit die Arbeiten von Richert (19), Halberstam (9) und Hua (12) zusammenzufassen und zu verallgemeinern. Dabei sind $b_1, \ldots, b_s$ ganze positive Zahlen mit $(b_1, \ldots, b_s) = 1$, und die $f_j(x)$ sind Polynome in x vom Grade $k_j \geqq 2$ mit ganzen Koeffizienten, den jeweils höchsten Koeffizienten als positiv vorausgesetzt.

In der ganzen Arbeit soll N stets eine genügend große ganze Zahl sein, ohne daß dies jedes Mal ausdrücklich hervorgehoben wird.

I. Abschnitt: Bekannte Sätze.

Satz I, 1: Eulersche Summenformel.

Sei $g(z)$ eine in $0 < a \leqq z \leqq \beta$ stetig differenzierbare (reelle oder komplexe) Funktion; sei a ganz. Dann ist:

$$(1) \qquad \sum_{a \leqq n \leqq \beta} g(n) = \int_a^\beta g(z)\,dz + \int_a^\beta (z - [z])\, g'(z)\,dz + g(a) - (\beta - [\beta]) \cdot g(\beta).$$

Ist in $a \leqq z \leqq \beta$ stets $g'(z) \leqq 0$ oder $g'(z) \geqq 0$, so gilt:

$$(2) \qquad \sum_{a \leqq n \leqq \beta} g(n) = \int_a^\beta g(z)\,dz + O(|g(a)| + |g(\beta)|).$$

[2]) Das Literaturverzeichnis für Teil I und II befindet sich am Ende von Teil I.

Satz I, 2: Abelsche Summation.

Sei die reelle Zahlenfolge $\{\lambda_\nu;\ \nu = 1, 2, \ldots\}$ *mit* $\lambda_1 \leqq \lambda_2 \leqq \lambda_3 \leqq \cdots$ *und* $\lim\limits_{n\to\infty} \lambda_n = \infty$ *gegeben. In* $\lambda_1 \leqq z \leqq \beta$ *sei* $g(z)$ *eine stetig differenzierbare (reelle oder komplexe) Funktion. Dann ist, wenn die* α_n *beliebige komplexe Zahlen sind:*

$$(3) \qquad \sum_{\lambda_1 \leqq \lambda_n \leqq \beta} \alpha_n \cdot g(\lambda_n) = \mathsf{A}(\beta) \cdot g(\beta) - \int_{\lambda_1}^{\beta} \mathsf{A}(z) \cdot g'(z)\, dz.$$

Dabei haben wir zur Abkürzung $\mathsf{A}(z) = \sum\limits_{\lambda_1 \leqq \lambda_n \leqq z} \alpha_n$ *gesetzt.*

(Prachar (18), S. 372 und 371, Satz 1. 5 bzw. 1. 4).

Satz I, 3: „Additionstheorem".

Es sei $f(z)$ *eine in* $0 \leqq z < \infty$ *stetig differenzierbare reell-wertige Funktion; sei mit reellen oder komplexen Koeffizienten* λ_x

$$(4) \qquad F(\alpha, R) = \sum_{0 \leqq x \leqq R} \lambda_x \cdot e(\alpha \cdot f(x)).$$

Dann gilt:

$$(5) \quad F(\alpha_1 + \alpha_2, P) = e\big(\alpha_2 f(P)\big) \cdot F(\alpha_1, P) - 2\pi i \alpha_2 \cdot \int_0^P e\big(\alpha_2 f(z)\big) \cdot f'(z) \cdot F(\alpha_1, z)\, dz.$$

Estermann (7), S. 53, beweist das Additionstheorem für den Spezialfall $f(z) = z$.

Beweis: Wir haben für $0 \leqq \beta \leqq \gamma$:

$$(6) \qquad \int_\beta^\gamma 2\pi i \alpha_2 \cdot f'(z) \cdot e\big(\alpha_2 f(z)\big)\, dz = e\big(\alpha_2 f(\gamma)\big) - e\big(\alpha_2 f(\beta)\big).$$

Demnach ist mit (4) und (6):

$$(7) \quad F(\alpha_1 + \alpha_2, P) = \sum_{0 \leqq x \leqq P} \lambda_x \cdot e\big(\alpha_1 f(x)\big) \cdot \left\{ e(\alpha_2 f(P)) - 2\pi i \alpha_2 \cdot \int_x^P e(\alpha_2 f(z)) \cdot f'(z) dz \right\}.$$

Wegen Satz I, 2 mit $\mathsf{A}(z) = \sum\limits_{0 \leqq x \leqq z} \lambda_x \cdot e\big(\alpha_1 f(x)\big)$ und $g(z) = -2\pi i \alpha_2 \cdot \int_z^P e(\alpha_2 f(z)) \cdot f'(z)\, dz$ folgt:

$$-\sum_{0 \leqq x \leqq P} \lambda_x \cdot e\big(\alpha_1 f(x)\big) \cdot 2\pi i \alpha_2 \cdot \int_x^P e\big(\alpha_2 f(z)\big) \cdot f'(z)\, dz$$
$$= \mathsf{A}(P) \cdot g(P) - 2\pi i \alpha_2 \cdot \int_0^P e\big(\alpha_2 f(z)\big) \cdot f'(z) \cdot \sum_{0 \leqq x \leqq z} \lambda_x \cdot e\big(\alpha_1 f(x)\big)\, dz.$$

Hieraus folgt mit (7) und wegen $g(P) = 0$ die Behauptung (5).

Satz I, 4: Primzahlsatz.

Sei A *eine beliebige positive, aber fest vorgegebene Zahl, sei* $P \geqq 3$, *sei* $(q, x) = 1$ *und* $q \leqq \log^A P$. *Für*

$$(8) \qquad \pi(P; q, x) = \sum_{\substack{p \equiv x \bmod q \\ p \leqq P,}} 1$$

gilt dann: Es gibt eine positive Konstante c_1, *so daß*

$$(9) \qquad \pi(P; q, x) = \frac{\mathrm{li}\, P}{\varphi(q)} + O\left(P \cdot \exp\left(-c_1 \cdot \sqrt{\log P}\right)\right)$$

ist.

Dabei ist

$$\text{(10)} \qquad \text{ls}\, P = \sum_{m=2}^{P} \frac{1}{\log m}$$

gesetzt worden.

Für c_1 kann z. B. $c_1 = \frac{1}{200}$ gewählt werden.

Beweis: z. B. Estermann (7), Theorem 55, Seite 51.

Nun folgen drei für uns später wichtige Abschätzungen von Exponentialsummen.

Satz I, 5: *Sei* $\alpha = \frac{a}{q} + \frac{\lambda}{q^2}$ *mit* $(a, q) = 1$, $|\lambda| \leqq 1$ *und* $0 < Q \leqq q \leqq \frac{N}{Q}$. *Weiter gelte für die ganze Zahl* m: $0 < m \leqq Q^{\frac{1}{3}}$. *Dann ist für jedes* $\varepsilon > 0$

$$\text{(11)} \qquad \left| \sum_{p \leqq N} e(\alpha m p) \right| \ll N \cdot \log N \cdot Q^{-\frac{1}{6}+\varepsilon}.$$

(Vinogradov (26)).

Satz I, 6: *Sei* $f(x) = \alpha \cdot x^k + \alpha_1 \cdot x^{k-1} + \cdots + \alpha_k$ *ein Polynom mit reellen Koeffizienten vom Grade* $k \geqq 2$. *Sei* $\alpha = \frac{a}{q} + \frac{\lambda}{q^2}$ *mit* $|\lambda| \leqq 1$, $q > 0$ *und* $(a, q) = 1$. *Wir setzen*: $U = \min\left(N^{\frac{1}{3}}, q, \frac{N^k}{q}\right)$. *Es sei*

$$\text{(12)} \qquad U \geqq (\log N)^{(2k+1)\cdot 2^{6k-2}}.$$

Dann gilt mit einer nur von k *abhängigen Konstanten* $c_2(k)$:

$$\text{(13)} \qquad \left| \sum_{p \leqq N} e\big(m \cdot f(p)\big) \right| < c_2(k) \cdot N \cdot \left(m \cdot U^{-\frac{1}{4k+4}}\right)^{2^{-2k}}$$

(Vinogradov (25)).

Satz I, 7: *Sei* $f(x) = a_0 x^k + a_1 x^{k-1} + \cdots + a_{k-1} x$ *ein Polynom mit ganzen Koeffizienten; es sei* $(a, q) = 1$ *und* $(a_0, a_1, \ldots, a_{k-1}, q) = 1$. *Dann ist*:

$$\text{(14)} \qquad \left| \sum_{1 \leqq x \leqq q} e\left(\frac{a}{q} \cdot f(x)\right) \right| \leqq c_3(k, \varepsilon) \cdot q^{1-\frac{1}{k}+\varepsilon},$$

wobei $c_3(k, \varepsilon)$ *von* $a, a_0, \ldots, a_{k-1}$ *unabhängig ist* (Hua (14), Chap. I).

Zum Schluß fügen wir noch einen Satz arithmetischer Natur an:

Satz I, 8: *Sei* $F(x_1, \ldots, x_n)$ *ein Polynom in* n *Veränderlichen* $x_1, \ldots, x_n$ *vom Grade* k *mit ganzen Koeffizienten, deren größter gemeinsamer Teiler gleich* 1 *ist.* $T(|m|)$ *bezeichne die Anzahl der positiven Teiler von* $|m|$. l *sei eine ganze, positive Zahl.*

Wir setzen:

$$X = \max_{1 \leqq x_\nu \leqq P,\ \nu = 1, \ldots, n} |F(x_1, \ldots, x_n)|$$

$$Y = \max\left(P^n, X^{\frac{n}{k}}\right).$$

Dann ist unabhängig von den Koeffizienten des Polynoms $F(x_1, \ldots, x_n)$ *mit positiven Konstanten* c_4, c_5, *die nur von* k, l, n *abhängen*:

$$\sum_{\substack{x_1 = 1 \\ F(x_1, \ldots, x_n) \neq 0}}^{P} \cdots \sum_{x_n = 1}^{P} T^l\big(|F(x_1, \ldots, x_n)|\big) \leqq c_4(k, l, n) \cdot Y \cdot |\log X|^{c_5(k, l, n)}$$

(Hua (14), Chap. II).

II. Abschnitt: Darstellung großer ganzer Zahlen N durch Summen von Primzahlen und Primzahlpotenzen.

1. Formulierung des Hauptsatzes.

In diesem Abschnitt soll folgender Satz bewiesen werden:

Hauptsatz: *Gegeben seien die Polynome*

$$(1,1) \qquad f_j(x) = a_{0j}x^{k_j} + a_{1j}x^{k_j-1} + \cdots + a_{k_j,j} \qquad (j = 1, 2, \ldots, r)$$

vom Grade $k_j \geqq 2$ *mit ganzrationalen Koeffizienten* $a_{0j}, a_{1j}, \ldots, a_{k_j,j}$, *wobei* $a_{0j} > 0$ *sei.*

(1. 2) *Die Zahlen* $b_1, b_2, \ldots, b_s$ *seien ganzrational und positiv. Es sei* $(b_1, \ldots, b_s) = 1$.

N *sei, wie immer, eine hinreichend große ganze Zahl.* $p_1, \ldots, p_s, p'_1, \ldots, p'_r$ *bezeichnen Primzahlen, die folgenden Bedingungen genügen:*

$$(1,3) \qquad p_\sigma \leqq \frac{N}{b_\sigma}, \quad (\sigma = 1, 2, \ldots, s); \qquad p'_j \leqq P_j = \left[\sqrt[k_j]{\frac{N}{a_{0j}}}\right], \ (j = 1, 2, \ldots, r).$$

Wir setzen für $i < 0$ *formal* $a_{i,j} = 0$; *sei*

$$u_j = \sum_{w=0}^{\infty} a_{k_j - w\cdot(p-1),\, j} \qquad (j = 1, 2, \ldots, r).$$

Für jede Primzahl $p > 2$, *die in genau* $s - 1$ *der* b_σ $(\sigma = 1, 2, \ldots, s)$ *aufgeht, seien nicht alle folgenden Kongruenzen* mod p *erfüllt:*

$$(1,4) \qquad \begin{cases} u_1 + u_2 + \cdots + u_r \equiv N \bmod p \\ \textit{und} \\ \sum\limits_{w=0}^{\infty} a_{k_j - v - w(p-1),\, j} \equiv 0 \bmod p \end{cases}$$

für $v = 1, 2, \ldots, p-2$ *und* $j = 1, 2, \ldots, r$.

(1, 5) *Weiter sei* $s \geqq 2$ *und* $r \geqq 1$ *oder* $s \geqq 3$ *und* $r \geqq 0$.

(1, 6) *Im Falle* $r = 0$ *sei* N *zu je* $s - 1$ *der* b_σ $(\sigma = 1, \ldots, s)$ *teilerfremd.*

Gilt schließlich noch

$$(1,7) \qquad b_1 + \cdots + b_s + f_1(1) + \cdots + f_r(1) \equiv N \ \textit{mod}\ 2,$$

so ist N *in der Form*

$$(1,8) \qquad N = b_1 p_1 + \cdots + b_s p_s + f_1(p'_1) + \cdots + f_r(p'_r)$$

darstellbar.

Die Anzahl $r(N)$ *der Darstellungen ist:*

$$(1,9) \qquad r(N) = \mathfrak{S}(N) \cdot \varrho(N) + O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-(s+r)-B}\right).$$

Dabei wird $\varrho(N)$ *durch Satz* II, 5, *Formel* (3, 11) *oder* (3, 12) *oder* (3, 13) *gegeben.*

Die Singuläre Reihe $\mathfrak{S}(N)$ *wird durch die Formel* (2, 4) *des nächsten Paragraphen gegeben. Unter den angegebenen Voraussetzungen ist* $\mathfrak{S}(N) \geqq c_6$ *gleichmäßig für alle* $N > 0$, *die der Bedingung* (1, 7) *genügen und für die nicht alle Kongruenzen* (1, 4) *gelten, mit einer von* N *unabhängigen Konstanten* $c_6 > 0$.

Die in die O-Abschätzung eingehende Konstante B hängt von einem Parameter A ab, für den, wenn

$$(1,10) \qquad k = \max k_j \quad (j = 1, \ldots, r)$$

gesetzt wird, vorausgesetzt werde, daß

$$(1,11) \qquad A \geqq 1 + \max\{s + r;\ (2k+1)\cdot 2^{6k-2};\ 2^{2k}\cdot(4k+7)\cdot(2s+r-3)\}.$$

Durch geeignete Wahl von A läßt sich die Konstante B in der O-Abschätzung größer als jede vorgegebene Zahl machen. Die genaue Abhängigkeit $B = B(A)$ ist auf Seite 44 gegeben.

Anmerkung: Anwendungen des Hauptsatzes folgen auf Seite 45f.

Die im Hauptsatz eingeführten Bezeichnungen sowie die Voraussetzungen (1, 2) und (1, 5) sollen für den ganzen II. Abschnitt gelten.

2. Untersuchung der Singulären Reihe.

Wir setzen, wobei $\varphi(q)$ die Anzahl der zu q teilerfremden Restklassen mod q bezeichnet:

$$(2,1) \qquad W_{a,q,f_j} = \sum_{\substack{1 \leq x \leq q \\ (x,q)=1}} e\left(\frac{a}{q}\cdot f_j(x)\right); \qquad (a,q) = 1,\ j = 1, \ldots, r.$$

$$(2,2) \qquad D_q(a\cdot b_\sigma) = \sum_{\substack{1 \leq x \leq q \\ (x,q)=1}} e\left(\frac{a\cdot b_\sigma}{q}\cdot x\right); \qquad (a,q) = 1,\ \sigma = 1, \ldots, s.$$

$$(2,3) \qquad A(N,q) = (\varphi(q))^{-(r+s)}\cdot \sum_{\substack{1 \leq a \leq q \\ (a,q)=1}} \prod_{\sigma=1}^{s} D_q(b_\sigma)\cdot \prod_{j=1}^{r} W_{a,q,f_j}\cdot e\left(-\frac{a}{q}\cdot N\right)$$

$$(2,4) \qquad \mathfrak{S}(N) = \sum_{q=1}^{\infty} A(N,q).$$

Lemma 2.1: *Sei $f(x) = a_0x^k + a_1x^{k-1} + \cdots + a_k$ ein Polynom mit ganzen Koeffizienten, sei $(a,q) = 1$ und*

$$W_{a,q,f} = \sum_{\substack{1 \leq x \leq q \\ (x,q)=1}} e\left(\frac{a}{q}\cdot f(x)\right).$$

Dann gilt:

$$|W_{a,q,f}| \leqq c_7(k,\varepsilon)\cdot q^{1-\frac{1}{k}+\varepsilon}\cdot(a_0, a_1, \ldots, a_{k-1})^{\frac{1}{k}}$$

mit einer nur von k und ε abhängigen Konstanten $c_7 > 0$.

Beweis: Nach Vinogradov (28), Chap. IX, Lemma 2, ist

$$W_{a,q,f} = \sum_{\substack{d|q \\ d>0}} \mu(d)\cdot S_d \text{ mit } S_d = \sum_{1 \leq x \leq \frac{q}{d}} e\left(\frac{a}{q}\, f(xd)\right) = e\left(\frac{a}{q}\cdot a_k\right)\cdot \sum_{1 \leq x \leq \frac{q}{d}} e\left(\frac{a}{q}\,(f(xd) - a_k)\right).$$

Sei t der größte gemeinsame Teiler $t = (a_0d^k, a_1d^{k-1}, \ldots, a_{k-1}d, q)$. Wegen $d|q$ gilt $d|t$. Somit wird:

$$|S_d| = \left|\sum_{1 \leq x \leq \frac{q}{d}} e\left(\frac{a}{\frac{q}{t}}\cdot\left(\frac{a_0d^k}{t}\cdot x^k + \cdots + \frac{a_{k-1}d}{t}\cdot x\right)\right)\right|$$

$$= \frac{t}{d}\cdot\left|\sum_{1 \leq x \leq \frac{q}{t}} e\left(\frac{a}{\frac{q}{t}}\left(\frac{a_0d^k}{t}\cdot x^k + \cdots + \frac{a_{k-1}d}{t}\cdot x\right)\right)\right|.$$

Offensichtlich ist $t \leqq (a_0, a_1, \ldots, a_{k-1}) \cdot d^k$.

Wegen $\left(\frac{a_0 d^k}{t}, \ldots, \frac{a_{k-1} d}{t}, \frac{q}{t}\right) = 1$ können wir Satz I, 7 von Hua anwenden und erhalten:

$$|S_d| \leqq \frac{t}{d} \cdot c_3(k, \varepsilon') \cdot \left(\frac{q}{t}\right)^{1-\frac{1}{k}+\varepsilon'}$$

$$\leqq c_3(k, \varepsilon') \cdot q^{1-\frac{1}{k}+\varepsilon'} \cdot \frac{1}{d} \cdot t^{\frac{1}{k}} \leqq c_3(k, \varepsilon') \cdot q^{1-\frac{1}{k}+\varepsilon'} (a_0, a_1, \ldots, a_{k-1})^{\frac{1}{k}}.$$

Nach Landau (15), Satz 260, gilt für die Anzahl $T(q)$ der Teiler von q: $T(q) \leqq c'(\varepsilon') \cdot q^{\varepsilon'}$, also folgt aus $|W_{a,q,f}| \leqq \sum_{d|q} |S_d|$ unmittelbar die Behauptung.

Lemma 2. 2: *Mit* (2, 2) $D_q(l) = \sum_{\substack{1 \leqq x \leqq q \\ (x,q)=1}} e\left(\frac{l}{q} \cdot x\right)$, *$l$ ganz, ist:*

(2, 5) $$D_q(l) = \sum_{d|(l,q)} d \cdot \mu\left(\frac{q}{d}\right);$$

(2, 6) $$D_q(l) = \mu(q) \qquad \textit{für } (q, l) = 1.$$

(2, 7) $$D_q(bl) = D_q(b) \qquad \textit{für } (q, l) = 1.$$

(2, 8) $$D_{q_1}(l) \cdot D_{q_2}(l) = D_{q_1 q_2}(l) \qquad \textit{für } (q_1, q_2) = 1.$$

(2, 9) $$|D_q(l)| \leqq \varphi(q).$$

Sind $b_1, \ldots, b_s$ positive ganze Zahlen mit $(b_1, \ldots, b_s) = 1$, und ist

(2, 10) $$\delta_q = \prod_{\sigma=1}^{s} D_q(b_\sigma), \quad \textit{so ist:} \quad \text{a)} \quad \delta_q = 0 \qquad \textit{für } \mu(q) = 0$$

$$\text{b)} \quad |\delta_q| \leqq \prod_{\sigma=1}^{s} b_\sigma.$$

Beweis: Für (2, 5) bis (2, 9) siehe Richert (19), Lemma 5. Sei nun $\mu(q) = 0$, so ist $q = q_1^2 \cdot q_2$ mit $q_1 > 1$. Nehmen wir an, daß $\delta_q \neq 0$ ist, so ist für jedes $\sigma = 1, \ldots, s$ $D_q(b_\sigma) \neq 0$. Mit (2,5) ist

$$D_q(b_\sigma) = \sum_{d|(b_\sigma, q)} d \cdot \mu\left(\frac{q}{d}\right) = \sum_{\substack{d|(b_\sigma, q) \\ q_1|d}} d \cdot \mu\left(\frac{q}{d}\right),$$

weil für $q_1 \nmid d$ (und $d|q$) $\mu\left(\frac{q}{d}\right) = \mu\left(\frac{q_2 \cdot q_1^2}{d}\right) = 0$ ist. Also gibt es für jedes b_σ wenigstens ein d_σ mit $d_\sigma | (b_\sigma, q)$ und $q_1 | d_\sigma$, woraus $q_1 | (b_1, \ldots, b_s)$ folgt, also $q_1 | 1$ im Gegensatz zu $q_1 > 1$. Somit ist die Annahme $\delta_q \neq 0$ für $\mu(q) = 0$ falsch und (2, 10a) ist bewiesen.

Nach (2, 8) ist δ_q multiplikativ, also ist unter Beachtung von (2, 5) und (2, 10a):

$$|\delta_q| \leqq \left| \prod_{\sigma=1}^{s} \prod_{p|q} D_p(b_\sigma) \right| \leqq \left| \prod_{\sigma=1}^{s} \prod_{p|(b_\sigma, q)} (p-1) \right| \leqq \prod_{\sigma=1}^{s} b_\sigma = O(1).$$

Lemma 2. 3: *Für das durch* (2, 3) *erklärte $A(N, q)$ gilt:*

(2, 11) $$|A(N, q)| \leqq c_{10}(k, \varepsilon, r, s, b_1, \ldots, b_s)\, q^{-(s-1)-\frac{r}{k}+\varepsilon}.$$

Die Singuläre Reihe (2, 4) *ist absolut konvergent und es ist für $A > 0$*

(2, 12) $$\left| \mathfrak{S}(N) - \sum_{1 \leqq q \leqq \log^A N} A(N, q) \right| = \left| \sum_{q > \log^A N} A(N, q) \right| = O\left((\log N)^{-\frac{A}{2 \max(1, k)}}\right).$$

Beweis: Aus (2, 3) folgt mit (2, 10) und Lemma 2. 1 unter Berücksichtigung von $(\varphi(q))^{-1} \leqq c_8(\varepsilon') \cdot q^{\varepsilon'-1}$

$$|A(N,q)| \leqq c_8^s \cdot q^{-s+\varepsilon' \cdot s} \cdot q \cdot \prod_1^s b_\sigma \cdot c_7^r \cdot q^{-\frac{r}{k}+r\varepsilon''} \leqq c_9(r,k,\varepsilon,s) \cdot \prod_1^s b_\sigma \cdot q^{-(s-1)-\frac{r}{k}+\varepsilon}.$$

Wegen (1, 5) ist also $A(N,q) \ll q^{-(1+\eta)}$ mit $\eta > 0$, woraus die absolute Konvergenz der Singulären Reihe folgt.

(2, 12) folgt unmittelbar aus (2, 11).

Lemma 2. 4: *Die zahlentheoretische Funktion $h(q)$ sei multiplikativ und $\sum_{q=1}^{\infty} |h(q)|$ sei konvergent. Dann ist:*

$$\sum_{q=1}^{\infty} h(q) = \prod_{p \geqq 2} \left(\sum_{m=0}^{\infty} h(p^m) \right).$$

Vgl. z. B. Estermann (7), Satz 2.

Lemma 2. 5: *$A(N,q)$ ist multiplikativ, d. h. für $(q_1, q_2) = 1$ ist:*

$$A(N, q_1 q_2) = A(N, q_1) A(N, q_2).$$

Anmerkung: Für Lemma 2. 5 braucht nicht (1, 5) vorausgesetzt zu werden, es gilt vielmehr schon für $s \geqq 0$ und $r \geqq 0$.

Beweis: Die Bezeichnung $\sum'_{y \bmod q}$ (kurz $\sum'_y$) soll bedeuten, daß y ein reduziertes Restsystem modulo q durchläuft.

Sei nun $(q_1, q_2) = 1$. Durchlaufen a_1 bzw. a_2 je ein reduziertes Restsystem mod q_1 bzw. mod q_2, so durchläuft $a_1 q_2 + a_2 q_1$ ein reduziertes Restsystem mod $q_1 q_2$ (Landau (15) Satz 74). Wegen (2, 8), und weil $\varphi(q)$ multiplikativ ist, genügt es zu zeigen, daß

$$R(q) = \sum'_{a \bmod q} \prod_{j=1}^{r} W_{a,q,f_j} \cdot e\left(-\frac{a}{q} N\right) = \sum'_{a \bmod q} \sum'_{x_1, \ldots, x_r \bmod q} e\left(\frac{a}{q} (f_1(x_1) + \cdots + f_r(x_r) - N)\right)$$

multiplikativ ist. Denn es ist $A(N,q) = (\varphi(q))^{-(r+s)} \cdot \prod_{\sigma=1}^{s} D_q(b_\sigma) \cdot R_q$. Unter Benutzung der Taylorentwicklung des Polynoms $f_j(x_1 q_2 + x_2 q_1)$ an der Stelle $x_1 q_2$ bzw. $x_2 q_1$ ist:

$$\begin{aligned}
&\sum'_{x_1 \bmod q_1} \sum'_{x_2 \bmod q_2} e\left\{\frac{a_1 q_2 + a_2 q_1}{q_1 q_2} \cdot f_j(x_1 q_2 + x_2 q_1)\right\} \\
&= \sum'_{x_1, x_2} e\left\{\frac{a_1}{q_1} \cdot \left(f_j(q_2 x_1) + \frac{f'_j(q_2 x_1)}{1!} \cdot q_1 x_2 + \cdots\right) + \frac{a_2}{q_2} \cdot \left(f_j(q_1 x_2) + \frac{f'_j(q_1 x_2)}{1!} \cdot q_2 x_1 + \cdots\right)\right\} \\
&= \sum'_{x_1, x_2} e\left\{\frac{a_1}{q_1} \cdot f_j(q_2 x_1) + \frac{a_2}{q_2} \cdot f_j(q_1 x_2)\right\} = \sum'_{x \bmod q_1} \sum'_{y \bmod q_2} e\left(\frac{a_1}{q_1} f_j(x) + \frac{a_2}{q_2} f_j(y)\right) \\
&\qquad (j = 1, 2, \ldots, r).
\end{aligned}$$

Daraus folgt unmittelbar:

$$\begin{aligned}
R(q_1) \cdot R(q_2) &= \sum'_{a_1 \bmod q_1} \sum'_{a_2 \bmod q_2} \sum'_{x_1 \cdots x_r \bmod q_1} \sum'_{y_1 \cdots y_r \bmod q_2} e\left\{\frac{a_1}{q_1} \cdot (f_1(x_1) + \cdots + f_r(x_r) - N) \right. \\
&\qquad \left. + \frac{a_2}{q_2} (f_1(y_1) + \cdots + f_r(y_r) - N\right\} \\
&= \sum'_{a_1, a_2} \sum'_{x_1 \cdots x_r} \sum'_{y_1 \cdots y_r} e\left\{\frac{a_1 q_2 + a_2 q_1}{q_1 q_2} \cdot (f_1(x_1 q_2 + y_1 q_1) + \cdots + f_r(x_r q_2 + y_r q_1) - N)\right\} \\
&= \sum'_{a \bmod q_1 q_2} \sum_{z_1 \cdots z_r \bmod q_1 q_2} e\left(\frac{a}{q_1 q_2} \cdot (f_1(z_1) + \cdots + f_r(z_r) - N)\right) = R(q_1 q_2).
\end{aligned}$$

Lemma 2. 6:

$$(2,13)\qquad \mathfrak{S}(N) = \prod_{p \geqq 2} \{1 + A(N,p)\} = \prod_{p \geqq 2} \left\{1 + \frac{\prod_{\sigma=1}^{s} D_p(b_\sigma)}{(p-1)^{r+s}} \cdot \sum_{a=1}^{p-1} \prod_{j=1}^{r} W_{a,p,f_j} \cdot e\left(-\frac{a}{p} N\right)\right\}.$$

Beweis: Auf die durch (2, 4) gegebene unendliche Reihe wenden wir Lemma 2. 4 an, was auf Grund von Lemma 2. 3 und 2. 5 möglich ist. Wegen $(b_1, \ldots . b_s) = 1$ und (2, 10a) reduziert sich $\sum_{m=0}^{\infty} A(N, p^m)$ auf $1 + A(N, p)$, woraus Lemma 2. 6 folgt.

Lemma 2. 7: *Sei $M_p = M_p(N, f_1, \ldots, f_r)$ die Lösungsanzahl der Kongruenz*

$$(2,14)\qquad f_1(x_1) + \cdots + f_r(x_r) \equiv N \bmod p \text{ für } r \geqq 1$$

mit den Einschränkungen $1 \leqq x_j \leqq p-1$ $(j = 1, \ldots, r)$. Dann ist:

$$(2,15)\qquad A(N,p) = (p-1)^{-(r+s)} \cdot \prod_{\sigma=1}^{s} D_p(b_\sigma) \cdot \{p M_p - (p-1)^r\}.$$

Speziell ist für $p = 2$:

$$(2,16)\qquad A(N,2) = \left\{\begin{matrix} 1 \\ -1 \end{matrix} \text{ für } b_1 + \cdots + b_s + f_1(1) + \cdots + f_r(1) \begin{matrix} \equiv N \\ \not\equiv N \end{matrix} \bmod 2\right\}.$$

Beweis: Nach Vinogradov (28), Chapt. I, Lemma 5 ist

$$S = \sum_{1 \leqq x \leqq q} e\left(\frac{d}{q} \cdot x\right) = \begin{cases} q & \text{für } q \mid d \\ 0 & \text{für } q \nmid d \end{cases}.$$

Demnach wird:

$$\sum_{a=1}^{p} \sum_{x_1=1}^{p-1} \cdots \sum_{x_r=1}^{p-1} e\left(\frac{a}{p} \cdot (f_1(x_1) + \cdots + f_r(x_r) - N)\right) = p \cdot M_p$$

und es ist nach (2, 4):

$$A(N,p) = \frac{\prod_{\sigma=1}^{s} D_p(b_\sigma)}{(\varphi(p))^{r+s}} \cdot \left\{\sum_{a=1}^{p} \sum_{x_1=1}^{p-1} \cdots \sum_{x_r=1}^{p-1} e\left(\frac{a}{p}(f_1(x_1) + \cdots + f_r(x_r) - N)\right) - (p-1)^r\right\}.$$

Die Behauptung (2, 16) rechnet man sich aus (2, 3) aus.

Lemma 2. 8: *Falls p in genau ν der b_σ $(\sigma = 1, \ldots, s)$ aufgeht, ist:*

$$(2,17)\qquad \prod_{\sigma=1}^{s} D_p(b_\sigma) = (-1)^{s-\nu} \cdot (p-1)^\nu.$$

Wegen $(b_1, \ldots, b_s) = 1$ ist $0 \leqq \nu \leqq s-1$.

Beweis: Folgt aus (2, 5).

Satz II, 1: *Sei $f(x) = d_0 x^k + d_1 x^{k-1} + \cdots + d_k$ ein Polynom mit ganzen Koeffizienten $d_\varkappa$ vom Grade k. Sei $d_0 \neq 0$. Wir setzen formal $d_\varkappa = 0$ für $\varkappa < 0$. p sei eine Primzahl. Die Kongruenz $f(x) \equiv N \bmod p$ habe genau $p-1$ Lösungen x mit $1 \leqq x \leqq p-1$. Notwendig und hinreichend hierfür ist das Bestehen folgender Kongruenzen:*

$$(2,18)\qquad \begin{cases} \sum_{w=0}^{\infty} d_{k-w(p-1)} \equiv N \bmod p \\ \sum_{w=0}^{\infty} d_{k-v-w(p-1)} \equiv 0 \bmod p \quad \text{für } v = 1, 2, \ldots, (p-2). \end{cases}$$

Beweis: 1.) $x = 1, 2, \ldots, p-1$ seien Lösungen von $f(x) \equiv N \bmod p$. Nach Hardy-Wright (11), Theorem 119 ist

$$(2, 19) \qquad \sum_{1 \leq x \leq p-1} x^u \equiv -\varepsilon_u(p) \bmod p \quad \text{mit} \quad \varepsilon_u(p) = \begin{cases} 1 & \text{für } (p-1) \mid u \\ 0 & \text{sonst.} \end{cases}$$

Addieren wir die $p-1$ Kongruenzen $f(x) - N \equiv 0 \bmod p$ für $x = 1, 2, \ldots, p-1$, so folgt:

$$-d_0 \cdot \varepsilon_k(p) - d_1 \varepsilon_{k-1}(p) - \cdots - d_{k-1} \varepsilon_1(p) + (p-1)\, d_k - (p-1) \cdot N \equiv 0 \bmod p$$

oder mit (2, 19):

$$d_k + d_{k-(p-1)} + \cdots - N = \sum_{w=0}^{\infty} d_{k-w(p-1)} - N \equiv 0 \bmod p,$$

also die erste der Kongruenzbedingungen (2, 18). Die weiteren $p-2$ Kongruenzbedingungen folgen analog durch Addition der $p-1$ Kongruenzen

$$f(x) \cdot x^t - N \cdot x^t \equiv 0 \bmod p \ (x = 1, 2, \ldots, p-1),$$

wenn man t von 1 bis $p-2$ laufen läßt.

2.) Sei (2, 18) erfüllt und sei $1 \leqq x \leqq p-1$. Wir setzen

$$K_v = \sum_{w=0}^{\infty} d_{k-v-w(p-1)}\, x^{v+w(p-1)} \quad \text{für } v = 0, 1, \ldots, p-2.$$

Dann ist auf Grund des kleinen Fermatschen Satzes

$$K_v \equiv x^v \cdot \sum_{w=0}^{\infty} d_{k-v-w(p-1)} \cdot (x^{p-1})^w \equiv x^v \cdot \sum_{w=0}^{\infty} d_{k-v-w(p-1)} \bmod p.$$

Mit (2, 18) folgt: $K_0 \equiv N \bmod p$, $K_v \equiv 0 \bmod p$ für $v = 1, 2, \ldots, p-2$.

Somit ist für $x = 1, 2, \ldots, p-1$:

$$f(x) = \sum_{v=0}^{p-2} K_v \equiv N \bmod p.$$

Korollar: *Die Kongruenz* $x^k \equiv N \bmod p$ *hat genau dann* $p-1$ *Lösungen* x *mit* $1 \leqq x \leqq p-1$, *wenn* $(p-1) \mid k$ *und* $N \equiv 1 \bmod p$ *ist.*

Satz II, 2: *Sei* p *Primzahl,* r *ganz,* $r \geqq 1$. *Mit den Bezeichnungen* (1, 1) *gilt: Die Kongruenz*

$$(2, 20) \qquad f_1(x_1) + \cdots + f_r(x_r) \equiv N \bmod p$$

hat genau dann $(p-1)^r$ *Lösungen* $x_1, \ldots, x_r$ *mit* $1 \leqq x_j \leqq p-1$ $(j = 1, \ldots, r)$, *wenn folgende Kongruenzen erfüllt sind:*

$$(2, 21) \qquad \begin{cases} \sum\limits_{1 \leq j \leq r} u_j \equiv N \bmod p & \textit{und} \\ \sum\limits_{w=0}^{\infty} a_{k_j - v - w(p-1), j} \equiv 0 \bmod p & \textit{für } \begin{matrix} v = 1, 2, \ldots, p-2, \\ j = 1, 2, \ldots, r. \end{matrix} \end{cases}$$

Dabei haben wir formal $a_{i,j} = 0$ *gesetzt für* $i < 0$, *und*

$$u_j = \sum_{w=0}^{\infty} a_{k_j - w(p-1), j} \qquad (j = 1, \ldots, r).$$

Beweis: Daß die Bedingung (2, 21) hinreichend ist, ist nach Satz II, 1 klar. Denn jede einzelne Kongruenz $f_j(x_j) \equiv u_j \bmod p$ hat $p-1$ Lösungen x_j mit $1 \leqq x_j \leqq p-1$, und es ist $\sum\limits_{j=1}^{r} u_j \equiv N \bmod p$. Um die Notwendigkeit zu beweisen, verfahren wir wie in

Satz II, 1. Die Kongruenz (2, 20) habe also $(p-1)^r$ Lösungssysteme $x_1, \ldots, x_r$ mit $1 \leqq x_j \leqq p-1$. Die Addition der $(p-1)$ Kongruenzen

$$f_1(x) + \cdots + f_r(x) \equiv N \bmod p \quad (x = 1, 2, \ldots, p-1)$$

gibt — wie in Satz II, 1 — die erste der Kongruenzbedingungen (2, 21). Die weiteren $r \cdot (p-2)$ Bedingungen folgen durch Addition der $(p-1)$ Kongruenzen (bei festem t und v)

$$\left(\sum_{\substack{j=1\\ j \neq t}}^{r} f_j(x_j)\right) \cdot x_t^v + f_t(x_t) \cdot x_t^v - N \cdot x_t^v \equiv 0 \bmod p \qquad (x_t = 1, \ldots, p-1),$$

wenn man dann t von 1 bis r und v von 1 bis $p-2$ laufen läßt.

Satz II, 3: *Sei $s \geqq 2$, $r \geqq 1$, $(b_1, \ldots, b_s) = 1$. Sei*

$$b_1 + \cdots + b_s + f_1(1) + \cdots + f_r(1) \equiv N \bmod 2.$$

Die Kongruenz $f_1(x_1) + \cdots + f_r(x_r) \equiv N \bmod p$ habe weniger als $(p-1)^r$ Lösungen $(x_1, \ldots, x_r)$ mit $1 \leqq x_j \leqq p-1$ für alle die Primzahlen p, die in genau $s-1$ der b_σ $(\sigma = 1, \ldots, s)$, aufgehen. Dann gibt es eine von N unabhängige Konstante $c_{12} > 0$, so daß

$$\mathfrak{S}(N) \geqq c_{12} > 0 \tag{2, 22}$$

gilt.

Beweis: Sei (1, 10) $k = \max k_j$. Nach (2, 11) ist $|A(N, p)| \leqq c_{10} \cdot p^{-1-\frac{1}{2k}}$ mit einer von N unabhängigen Konstanten c_{10}. Somit ist das absolut konvergente Produkt

$$\prod_{p > (2c_{10})^{4k}} (1 + A(N, p)) > \prod_{p > (2c_{10})^{4k}} \left(1 - \frac{1}{2} p^{-1-\frac{1}{4k}}\right) \geqq c_{11} > 0.$$

Es genügt nun der Nachweis, daß kein Faktor mit $p \leqq (2 \cdot c_{10})^{4k}$ in der durch (2, 13) gegebenen Produktdarstellung von $\mathfrak{S}(N)$ verschwindet, um (2, 22) zu beweisen. Für $p = 2$ ist $1 + A(N, 2) = 2 \neq 0$ wegen (2, 16). Sei nun $p > 2$ und p gehe in genau $s-1$ der b_σ auf. Nach Voraussetzung ist für diese p die Lösungsanzahl M_p (vgl. Lemma 2. 7) $M_p \leqq (p-1)^r - 1$. Also ist nach Lemma 2. 7 und 2. 8 (mit $\nu = s-1$):

$$\begin{aligned} |A(N, p)| &\leqq \frac{(p-1)^{s-1}}{(p-1)^{r+s}} \cdot \{p \cdot ((p-1)^r - 1) - (p-1)^r\} \\ &= (p-1)^{-(r+1)} \cdot \{(p-1)^{r+1} - p\} = 1 - p \cdot (p-1)^{-(r+1)} < 1. \end{aligned}$$

Geht p höchstens in $(s-2)$ der b_σ auf $(\sigma = 1, \ldots, s)$, so ist nach Lemma 2. 7 und 2. 8:

$$|A(N, p)| \leqq \frac{(p-1)^{s-2}}{(p-1)^{r+s}} \cdot \left\{p \cdot (p-1)^r - (p-1)^r\right\} = \frac{1}{p-1} < 1,$$

also jeweils $1 + A(N, p) > 0$.

Satz II, 3′: *Sei $s \geqq 3$ und $r = 0$. Sei $b_1 + \cdots + b_s \equiv N \bmod 2$, $(b_1, \ldots, b_s) = 1$ und N zu je $s-1$ der b_σ $(\sigma = 1, \ldots, s)$ teilerfremd. Dann gibt es eine von N unabhängige Konstante $c'_{12} > 0$, so daß*

$$\mathfrak{S}(N) \geqq c'_{12} \tag{2, 22′}$$

ist.

Beweis: Wie beim Beweise von Satz II, 3 genügt es, zu zeigen, daß kein Faktor mit „kleinem" p in der Produktdarstellung von $\mathfrak{S}(N)$ verschwindet. Für $p = 2$ folgt dies aus (2, 16). Sei also $p > 2$. Nun ist

$$A(N, p) = \frac{1}{(p-1)^s} \cdot \prod_{\sigma=1}^{s} D_p(b_\sigma) \cdot \sum_{a=1}^{p-1} e\left(-\frac{a}{p} \cdot N\right).$$

Geht p in höchstens $s-2$ der b_σ auf, so ist nach Lemma 2. 8:

$$\left|\prod_{\sigma=1}^{s} D_p(b_\sigma)\right| \leqq (p-1)^{s-2}, \quad \text{also} \quad |A(N,p)| \leqq \frac{1}{(p-1)} \quad \text{und} \quad 1 + A(N,p) > 0.$$

Geht p in genau $s-1$ der b_σ auf, so ist zwar $\left|\prod_{\sigma=1}^{s} D_p(b_\sigma)\right| = (p-1)^{s-1}$, aber weil N zu je $s-1$ der b_σ teilerfremd ist, so gilt $p \nmid N$, und deswegen $\left|\sum_{1 \leqq a \leqq p-1} e\left(-\frac{a}{p} \cdot N\right)\right| = 1$ (vgl. Lemma 2. 7), also $|A(N,p)| \leqq \frac{1}{p-1}$.

3. Lösungsanzahl einer diophantischen Gleichung.

Satz II, 4: *Seien* $f_j(x) = a_{0,j} \cdot x^{k_j} + a_{1,j} x^{k_j - 1} + \cdots + a_{k_j, j}$ *Polynome vom Grade* $k_j \geqq 2$ *mit ganzrationalen Koeffizienten* $a_{\nu, j}$, *wobei* $a_{0,j} > 0$ *sei* $(j = 1, \ldots, r)$. $b_1, \ldots, b_s$ *seien ganze, positive Zahlen mit* $(b_1, \ldots, b_s) = 1$. L *bezeichne die Lösungsanzahl der diophantischen Gleichung*

$$(3,1) \qquad b_1 m_1 + \cdots + b_s m_s + f_1(m_1') + \cdots + f_r(m_r') = N$$

in ganzen Zahlen m_σ, m_j' *mit*

$$0 \leqq m_\sigma \leqq N \cdot b_\sigma^{-1} \quad (\sigma = 1, \ldots, s); \qquad 0 \leqq m_j' \leqq (N \cdot a_{0j}^{-1})^{\frac{1}{k_j}} \quad (j = 1, \ldots, r).$$

Dann ist:

$$(3,2) \qquad L = \frac{E_r}{(s-1)!} \cdot \frac{a_{01}^{-\frac{1}{k_1}} \cdots a_{0r}^{-\frac{1}{k_r}}}{b_1 b_2 \cdots b_s} \cdot N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} + O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}-\frac{1}{k^*}}\right).$$

Dabei ist: $k^* = \max(1, k_1, \ldots, k_r)$;

$$\mathsf{B}(\alpha, \beta) = \frac{\Gamma(\alpha) \cdot \Gamma(\beta)}{\Gamma(\alpha+\beta)} \quad \textit{bezeichnet die Beta-Funktion.}$$

$$E_r = \prod_{0 \leqq j \leqq r-1} e_j, \quad e_0 = \frac{1}{k_1} \cdot \mathsf{B}\left(\frac{1}{k_1}, s\right), \quad e_j = \frac{1}{k_{j+1}} \cdot \mathsf{B}\left(\frac{1}{k_{j+1}}, s + \frac{1}{k_1} + \cdots + \frac{1}{k_j}\right).$$
$$(j = 1, \ldots, r-1).$$

Anmerkung: Die in die O-Abschätzung eingehenden Konstanten können von $k_1, \ldots, k_r$, $a_{\nu,j}$, b_σ, r und s abhängen, sind aber natürlich von N unabhängig.

Zum Beweise dieses Satzes benötigen wir einige Hilfssätze.

Lemma 3. 1: *Seien* $b_1, \ldots, b_s$ *ganze, positive Zahlen; sei* $d = (b_1, \ldots, b_s)$ *ihr größter gemeinsamer Teiler. Dann ist für* $s \geqq 1$ *die Lösungsanzahl* $L_s(Q)$ *der diophantischen Gleichung*

$$b_1 m_1 + \cdots + b_s m_s = Q$$

in ganzen, nichtnegativen Zahlen $m_1, \ldots, m_s$ *gegeben durch*

$$(3,3) \qquad L_s(Q) = \begin{cases} 0, & \textit{falls } d \nmid Q \\ \dfrac{1}{(s-1)!} \cdot \dfrac{d}{b_1 \cdots b_s} \cdot Q^{s-1} + O(Q^{s-2}), & \textit{falls } d \mid Q. \end{cases}$$

Beweis:* $L_s(Q) = 0$ für $d \nmid Q$ ist offensichtlich.

---

*) Lemma 3. 1 wurde im Spezialfall $s = 2$ von *Evelyn-Linfoot* in ihrer Arbeit: On a problem in the additive theory of numbers, II (Crelles Journal **164** (1931), S. 131–140) bewiesen.

Sei nun $d \mid Q$.

Wir setzen $b_\sigma = b'_\sigma d$, $(\sigma = 1, \ldots, s)$, $Q = Q' \cdot d$. Bezeichnet $L'_s(Q')$ die Lösungsanzahl der diophantischen Gleichung

$$b'_1 m_1 + \cdots + b'_s m_s = Q',$$

so ist $L_s(Q) = L'_s(Q')$.

Nehmen wir Lemma 3. 1 für $d = 1$ als bewiesen an, so ist wegen $(b'_1, \ldots, b'_s) = 1$ demnach

$$L_s(Q) = \frac{1}{(s-1)!} \cdot \frac{Q'^{s-1}}{b'_1 \cdots b'_s} + O(Q'^{s-2}) = \frac{1}{(s-1)!} \cdot \frac{Q^{s-1} \cdot d}{b_1 \cdots b_s} + O(Q^{s-2}).$$

Wir können also o. B. d. A. $d = 1$ voraussetzen.

Wir führen den Beweis durch vollständige Induktion nach s. Für $s = 1$ ist Lemma 3.1 trivial. Sei nun $s > 1$ und Lemma 3. 1 für $s - 1$ richtig. Wir setzen $D = (b_1, \ldots, b_{s-1})$; die diophantische Gleichung (*) $b_1 m_1 + \cdots + b_{s-1} m_{s-1} = Q - b_s m_s$ ist bei festem m_s genau für $D \mid (Q - b_s m_s)$ lösbar und hat dann nach Induktionsannahme

$$L_{s-1}(Q - b_s m_s) = \frac{1}{(s-2)!} \cdot \frac{D \cdot (Q - b_s m_s)^{s-2}}{b_1 \cdots b_{s-1}} + O(Q^{s-3})$$

Lösungen.

Durch den Ansatz $Q = R + Y \cdot b_s$ bestimmen wir ganze Zahlen $Y = \left[\frac{Q}{b_s}\right]$ und R mit $0 \leqq R < b_s$.

Wegen $(D, b_s) = 1$ ist die Kongruenz $b_s \cdot x \equiv Q' \bmod D$ eindeutig lösbar, also durchlaufen für jede ganze Zahl β die Zahlen $\beta, \beta + b_s, \beta + 2 \cdot b_s, \ldots, \beta + (D-1) \cdot b_s$ genau alle Reste modulo D.

Unter den $Y + 1$ Zahlen $(Q - b_s m_s)$, $\left(0 \leqq m_s \leqq \frac{Q}{b_s}\right)$, die wir jetzt in der Form

$$R, R + b_s, R + 2b_s, \ldots, R + Y \cdot b_s = Q$$

aufschreiben, sind somit, da genau unter D aufeinanderfolgenden Zahlen einmal der Rest 0 auftritt, genau

$$\frac{Y}{D} + O(1) = \frac{Q}{b_s \cdot D} + O(1)$$

durch D teilbare Zahlen, und genau für diese ist (*) lösbar.

Durch Summation über alle Werte von m_s, für die (*) lösbar ist, erhalten wir für die Lösungsanzahl $L_s(Q)$ von (3, 3) die Schranken:

$$L_s(Q) \leqq \frac{1}{(s-2)!} \cdot \frac{D}{b_1 \cdots b_{s-1}} \cdot \sum_{y=0}^{\left[\frac{Y}{D}\right]+1} (R + (D-1)\, b_s + y \cdot D \cdot b_s)^{s-2} + O(Y \cdot Q^{s-3}),$$

und

$$L_s(Q) \geqq \frac{1}{(s-2)!} \cdot \frac{D}{b_1 \cdots b_{s-1}} \cdot \sum_{y=0}^{\left[\frac{Y}{D}\right]} (R + y \cdot D \cdot b_s)^{s-2} + O(Y \cdot Q^{s-3}).$$

Die Ausrechnung ergibt wegen $\left[\frac{Y}{D}\right] = \frac{Q}{b_s D} + O(1)$ und

$$\sum_{y=0}^{\left[\frac{Y}{D}\right]} (R + y \cdot D \cdot b_s)^{s-2} = \frac{1}{s-1} \cdot D^{s-2} \cdot b_s^{s-2} \cdot \frac{Q^{s-1}}{(b_s D)^{s-1}} + O(Q^{s-2})$$

die Beziehung

$$L_s(Q) = \frac{1}{(s-1)!} \cdot \frac{Q^{s-1}}{b_1 \cdots b_s} + O(Q^{s-2}).$$

Lemma 3. 2: *Seien* $g_t(x) = a_{0,t} \cdot x^{k_t}$ $(t = 1, \ldots, T,\ T \geqq 0$ *ganz) Polynome mit ganzen Koeffizienten vom Grade* $k_t > 0$. *Sei* $a_{0,t} > 0$. $b_1, \ldots, b_s$ *seien ganze, positive Zahlen mit* $(b_1, \ldots, b_s) = 1$. *Die Lösungsanzahl der diophantischen Gleichung*

$$b_1 m_1 + \cdots + b_s m_s + g_1(m_1') + \cdots + g_T(m_T') = N \tag{3, 4}$$

in ganzen, nichtnegativen Zahlen $m_1, \ldots, m_s, m_1', \ldots, m_T'$ *ist dann*

$$L_T = \frac{A_T}{(s-1)! \cdot b_1 \cdots b_s} \cdot E_T \cdot N^{K_T} + O\left(N^{K_T - \frac{1}{k^*}}\right). \tag{3, 5}$$

Dabei ist zur Abkürzung gesetzt:

$$\left\{\begin{array}{l} A_0 = 1, \quad A_t = \left(a_{0,1}^{\frac{1}{k_1}} \cdot a_{0,2}^{\frac{1}{k_2}} \cdots a_{0,t}^{\frac{1}{k_t}}\right)^{-1}, \qquad t = 1, 2, \ldots, T. \\ K_0 = s - 1, \quad K_t = s - 1 + \dfrac{1}{k_1} + \cdots + \dfrac{1}{k_t}. \\ e_0 = \dfrac{1}{k_1} \cdot \mathsf{B}\left(\dfrac{1}{k_1}, K_0 + 1\right), \quad e_t = \dfrac{1}{k_{t+1}} \cdot \mathsf{B}\left(\dfrac{1}{k_{t+1}}, K_t + 1\right). \\ E_t = e_0 \cdot e_1 \cdots e_{t-1}, \quad (t \geqq 1), \quad E_0 = 1. \\ k^* = \max(1, k_1, \ldots, k_T). \end{array}\right. \tag{3, 6}$$

Beweis: Durch vollständige Induktion. Die Behauptung ist nach Lemma 3. 1 richtig für $T = 0$:

$$L_0 = \frac{1}{(s-1)!} \cdot \frac{N^{s-1}}{b_1 \cdots b_s} + O(N^{s-2}).$$

Wir nehmen an, die Behauptung sei richtig für $t - 1$ $(t \leqq T)$.

Nach Induktionsannahme ist die Lösungsanzahl $L_t(m_t')$ von

$$b_1 m_1 + \cdots + b_s m_s + g_1(m_1') + \cdots + g_{t-1}(m_{t-1}') = N - g_t(m_t')$$

bekannt, und zwar

$$L_t(m_t') = \frac{E_{t-1} \cdot A_{t-1}}{b_1 \cdots b_s \cdot (s-1)!} \cdot (N - g_t(m_t'))^{K_{t-1}} + O\left(N^{K_{t-1} - \frac{1}{k^*}}\right). \tag{3, 7}$$

Die Lösungsanzahl L_t von

$$b_1 m_1 + \cdots + b_s m_s + g_1(m_1') + \cdots + g_t(m_t') = N$$

ergibt sich aus (3, 7) durch Summation über alle Möglichkeiten für m_t'.

$$\begin{aligned} L_t &= \sum_{0 \leqq m_t' \leqq (N \cdot a_{0,t}^{-1})^{\frac{1}{k_t}}} \{L_t(m_t')\} \\ &= \frac{E_{t-1} \cdot A_{t-1}}{(s-1)!\, b_1 \cdots b_s} \cdot N^{K_{t-1}} \cdot \sum_{0 \leqq m_t' \leqq (N \cdot a_{0,t}^{-1})^{\frac{1}{k_t}}} \left(1 - \frac{a_{0,t} \cdot m_t'^{k_t}}{N}\right)^{K_{t-1}} + O\left(N^{K_{t-1} + \frac{1}{k_t} - \frac{1}{k^*}}\right). \end{aligned} \tag{3, 8}$$

Die Eulersche Summenformel (Satz I, 1) gibt:

$$\begin{aligned} \sum_{0 \leqq m_t' \leqq (N \cdot a_{0,t}^{-1})^{\frac{1}{k_t}}} \left(1 - \frac{a_{0,t} \cdot m_t'^{k_t}}{N}\right)^{K_{t-1}} &= \int_0^{(N \cdot a_{0,t}^{-1})^{\frac{1}{k_t}}} \left(1 - \frac{a_{0,t}\, z^{k_t}}{N}\right)^{K_{t-1}} dz + O(1) \\ &= \sqrt[k_t]{\frac{N}{a_{0,t}}} \cdot \int_0^1 (1 - \alpha^{k_t})^{K_{t-1}} d\alpha + O(1) = \sqrt[k_t]{\frac{N}{a_{0,t}}} \cdot \frac{1}{k_t} \cdot \mathsf{B}\left(\frac{1}{k_t}, K_{t-1} + 1\right) + O(1), \end{aligned}$$

nach Gröbner-Hofreiter (8), S. 179, Formel 1. Hieraus folgt mit (3, 8):

$$L_t = \frac{E_{t-1} \cdot A_{t-1}}{(s-1)! \cdot b_1 \cdots b_s} \cdot a_{0,t}^{-\frac{1}{k_t}} \cdot N^{K_t} \cdot \frac{1}{k_t} \cdot \mathrm{B}\left(\frac{1}{k_t}, K_{t-1}+1\right) + O\left(N^{K_t - \frac{1}{k^*}}\right)$$

$$= \frac{E_t \cdot A_t}{(s-1)!\, b_1 \cdots b_s} \cdot N^{K_t} + O\left(N^{K_t - \frac{1}{k^*}}\right).$$

Lemma 3. 3: *Seien $g'_t(x) = a_{0,t} \cdot x^{k_t} + \cdots + a_{k_t,t}$ Polynome mit ganzen Koeffizienten vom Grade $k_t > 0$; sei $a_{0,t} > 0$ $(t = 1, \ldots, T)$. Die Lösungsanzahl der diophantischen Gleichung*

$$(3, 9) \qquad b_1 m_1 + \cdots + b_s m_s + g'_1(m'_1) + \cdots + g'_T(m'_T) = N$$

in ganzen Zahlen $m_1, \ldots, m'_T \geqq 0$ ist dann:

$$(3, 10) \qquad L'_T = \frac{E_T \cdot A_T}{(s-1)! \cdot b_1 \cdots b_s} \cdot N^{K_T} + O\left(N^{K_T - \frac{1}{k^*}}\right).$$

Beweis: In (3, 9) schaffen wir die niederen Potenzen als die k_t-ten auf die rechte Seite und erhalten mit den Bezeichnungen von Lemma 3. 2 für jeden Lösungsvektor $m_1, \ldots, m_s, \ldots m'_T$ von (3, 9) mit passenden positiven Konstanten c' und c'' die beiden Ungleichungen:

$$b_1 m_1 + \cdots + b_s m_s + g_1(m'_1) + \cdots + g_T(m'_T) \leqq N + c' \cdot N^{1 - \frac{1}{k^*}},$$

bzw.

$$b_1 m_1 + \cdots + b_s m_s + g_1(m'_1) + \cdots + g_T(m'_T) \geqq N - c'' \cdot N^{1 - \frac{1}{k^*}}.$$

Somit liegt nach Lemma 3. 2 die Lösungsanzahl L'_T zwischen den Grenzen

$$\frac{E_T A_T}{(s-1)!\, b_1 \cdots b_s} \cdot \left(N - c'' \cdot N^{1 - \frac{1}{k^*}}\right)^{K_T} + O\left(N^{K_T - \frac{1}{k^*}}\right)$$

und

$$\frac{E_T A_T}{(s-1)!\, b_1 \cdots b_s} \cdot \left(N + c' \cdot N^{1 - \frac{1}{k^*}}\right)^{K_T} + O\left(N^{K_T - \frac{1}{k^*}}\right),$$

ist also gleich

$$L'_T = \frac{E_T A_T}{(s-1)!\, b_1 \cdots b_s} \cdot N^{K_T} + O\left(N^{K_T - \frac{1}{k^*}}\right).$$

Nun können wir Satz II, 4 beweisen:

Zu bestimmen ist die Lösungsanzahl L von

$$b_1 m_1 + \cdots + b_s m_s + f_1(m'_1) + \cdots + f_r(m'_r) = N.$$

Wir verwenden Lemma 3. 3 und setzen mit den Bezeichnungen (1, 1) und (1, 2) des Hauptsatzes für die $g'_t(x)$ aus Lemma 3. 3:

$$g'_1(x) = f_1(x), \ldots, g'_r(x) = f_r(x).$$

Dann ist

$$L = \frac{E_r \cdot A_r}{(s-1)!\, b_1 \cdots b_s} \cdot N^{K_r} + O\left(N^{K_r - \frac{1}{k^*}}\right)$$

mit

$$A_r = a_{0,1}^{-\frac{1}{k_1}} \cdots a_{0,r}^{-\frac{1}{k_r}}; \qquad k^* = \max(1, k_1, \ldots, k_r).$$

$$K_r = s - 1 + \frac{1}{k_1} + \cdots + \frac{1}{k_r};$$

$$E_r = \frac{1}{k_1 \cdots k_r} \cdot \prod_{j=1}^{r} \mathsf{B}\left(\frac{1}{k_j},\ s + \frac{1}{k_1} + \cdots + \frac{1}{k_{j-1}}\right).$$

Satz II, 5: *Sei*

$$(3,11) \quad \varrho(N) = \sum_{\substack{b_1 m_1 + \cdots + b_s m_s + f_1(m_1') + \cdots + f_r(m_r') = N \\ m_1 \geq 2, \ldots, m_s \geq 2,\ m_1' \geq 2, \ldots, m_r' \geq 2}} \frac{1}{\log m_1 \cdots \log m_s \cdot \log m_1' \cdots \log m_r'}.$$

Dann ist

$$(3,12) \qquad \varrho(N) = \frac{L}{(\log N)^{r+s}} \cdot k_1 \cdot k_2 \cdots k_r \cdot \left(1 + O\left(\frac{\log\log N}{\log N}\right)\right),$$

wobei L durch (3, 2) *gegeben wird.*

Beweis: Beschränken wir ein m_σ auf $m_\sigma \leqq N \cdot (\log N)^{-(r+s+1)}$, $\sigma = 1, \ldots, s$ oder ein m_j' auf $m_j' \leqq N^{\frac{1}{k_j}} \cdot (\log N)^{-(r+s+1)}$, $j = 1, \ldots, r$, so ist die Lösungsanzahl von

$$b_1 m_1 + \cdots + b_s m_s + f_1(m_1') + \cdots + f_r(m_r') = N$$

unter dieser einen Nebenbedingung offensichtlich kleiner als

$$N^{\frac{1}{k_1} + \cdots + \frac{1}{k_r} + s - 1} \cdot (\log N)^{-(r+s+1)} = O\left(L \cdot (\log N)^{-(r+s+1)}\right).$$

Somit ist:

$$\varrho(N) = \sum_{\substack{b_1 m_1 + \cdots + b_s m_s + f_1(m_1') + \cdots + f_r(m_r') = N \\ m_\sigma > N \cdot (\log N)^{-(r+s+1)};\ m_j' > N^{\frac{1}{k_j}} \cdot (\log N)^{-(r+s+1)}}} (\log m_1 \cdots \log m_s \cdot \log m_1' \cdots \log m_r')^{-1} + O\left(\frac{N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}}}{(\log N)^{r+s+1}}\right).$$

Diese Summe aber ist mit geeigneten Konstanten c_{13}, c_{14}:

$$\begin{aligned}
\varrho(N) &\leqq L \cdot \prod_{\sigma=1}^{s} \frac{1}{\log N - (r+s+1)\log\log N} \cdot \prod_{j=1}^{r} \frac{1}{\frac{1}{k_j}\log N - (r+s+1)\cdot\log\log N} \\
&\qquad + O\left(L \cdot (\log N)^{-(r+s+1)}\right) \\
&\leqq L \cdot \frac{k_1 \cdots k_r}{(\log N)^{r+s}} \cdot \left(1 + \frac{c_{13} \cdot \log\log N}{\log N}\right)^{s+r} + O\left(L \cdot (\log N)^{-(r+s+1)}\right) \\
&\leqq \left(1 + \frac{c_{14} \cdot \log\log N}{\log N}\right) \cdot \frac{L \cdot k_1 \cdots k_r}{(\log N)^{r+s}} + O\left(L (\log N)^{-(r+s+1)}\right).
\end{aligned}$$

Andererseits ist offensichtlich

$$\varrho(N) \geqq \frac{L \cdot k_1 \cdots k_r}{(\log N)^{r+s}}.$$

Also ist (mit (3, 2)):

$$(3,13) \quad \varrho(N) = \frac{1}{(s-1)!} \cdot \frac{k_1 \cdot k_2 \cdots k_r}{b_1 \cdot b_2 \cdots b_s} \cdot E_r \cdot a_{01}^{-\frac{1}{k_1}} \cdots a_{0r}^{-\frac{1}{k_r}} \frac{N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}}}{(\log N)^{r+s}} \cdot \left(1 + O\left(\frac{\log\log N}{\log N}\right)\right)$$

mit

$$E_r = \frac{1}{k_1 \cdots k_r} \cdot \mathsf{B}\left(\frac{1}{k_1}, s\right) \cdot \prod_{j=1}^{r-1} \mathsf{B}\left(\frac{1}{k_{j+1}}, \frac{1}{k_1} + \cdots + \frac{1}{k_j} + s\right).$$

4. Abschätzung in den Supplementintervallen.

Wir setzen mit den in (1, 1) und (1, 2) eingeführten Bezeichnungen:

$$P_j = \left[(N \cdot a_{0j}^{-1})^{\frac{1}{k_j}}\right] \qquad (j = 1, \ldots, r), \tag{4, 1}$$

$$F_\sigma(\alpha) = \sum_{p_\sigma \leq \frac{N}{b_\sigma}} e(\alpha \cdot b_\sigma p_\sigma) \qquad (\sigma = 1, 2, \ldots, s), \tag{4, 2}$$

$$F'_j(\alpha) = \sum_{p \leq P_j} e\big(\alpha \cdot f_j(p)\big) \qquad (j = 1, \ldots, r), \tag{4, 3}$$

$$F(\alpha) = F_1(\alpha) \cdots F_s(\alpha) \cdot F'_1(\alpha) \cdots F'_r(\alpha). \tag{4, 4}$$

A sei eine feste Zahl, für die (1, 11) gilt. Somit ist jedenfalls

$$A > (2k + 1) \cdot 2^{6k-2} \qquad (k = \max(k_1, \ldots, k_r)) \tag{4, 5}$$

erfüllt. Sei

$$\omega_0 = \frac{\log^A N}{N}. \tag{4, 6}$$

Dann ist die Darstellungsanzahl $r(N)$ von N in der Form

$$N = b_1 p_1 + \cdots + b_s p_s + f_1(p'_1) + \cdots + f_r(p'_r) \tag{1, 8}$$

gegeben durch

$$r(N) = \int_{-\omega_0}^{1-\omega_0} F(\alpha) \cdot e(-N\alpha)\, d\alpha. \tag{4, 7}$$

Das Integrationsintervall $[-\omega_0, 1 - \omega_0]$ teilen wir in bekannter Weise (ausführlich dargestellt z. B. in Prachar (18), S. 182f.) in Basis- und Supplement-Intervalle ein:

Jedem Bruch $\frac{a}{q}$ mit $(a, q) = 1$, $0 \leqq a < q$ und $0 < q \leqq \log^A N$ ordnen wir als Basisintervall das abgeschlossene Intervall

$$\mathfrak{M}_{a,q} = \left[\frac{a}{q} - \omega_0, \frac{a}{q} + \omega_0\right] \tag{4, 8}$$

zu. Da N als hinreichend groß vorausgesetzt ist, überlappen sich die einzelnen Basisintervalle nicht. Die Vereinigung der $\mathfrak{M}_{a,q}$ bezeichnen wir mit

$$\mathfrak{M} = \bigcup_{a,q} \mathfrak{M}_{a,q} = \sum_{1 \leq q \leq \log^A N} \sum_{\substack{0 \leq a \leq q-1 \\ (a,q)=1}} \mathfrak{M}_{a,q}.$$

Den Rest des Intervalles $[-\omega_0, 1 - \omega_0]$ nennen wir die Supplementintervalle $\mathfrak{m}$, also:

$$\mathfrak{m} = [-\omega_0, 1 - \omega_0] - \mathfrak{M}.$$

Wir bemerken: Ist $\alpha \in \mathfrak{m}$, so gibt es ein Zahlenpaar a, q mit $(a, q) = 1$ und $\log^A N < q \leqq N \cdot \log^{-A} N$, so daß $\left|\alpha - \frac{a}{q}\right| \leqq \frac{\log^A N}{q \cdot N}$ ist (Prachar (18), S. 184).

Es ist also:

$$r(N) = \int_{\mathfrak{m}} F(\alpha) \cdot e(-N\alpha)\, d\alpha + \sum_{q=1}^{\log^A N} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} \int_{\mathfrak{M}_{a,q}} F(\alpha) \cdot e(-N\alpha)\, d\alpha. \tag{4, 9}$$

Wir schätzen nun das Integral über die Supplementintervalle ab.

Lemma 4. 1: *Ist* $\alpha \in \mathfrak{m}$, *so ist:*

$$(4,10)\qquad \Big|\sum_{p \leq P_j} e\big(\alpha \cdot f_j(p)\big)\Big| = |F_j'(\alpha)| \ll N^{\frac{1}{k_j}} \cdot (\log N)^{-A_0} \quad mit\ A_0 = \frac{A}{2^{2k} \cdot (4k+4)}$$

$$(4,11)\qquad \Big|\sum_{p \leq \frac{N}{b_\sigma}} e(\alpha b_\sigma p)\Big| \ll N \cdot \log N \cdot (\log N)^{-\frac{A}{7}}.$$

Beweis: Satz I, 6 bzw. Satz I, 5.

Lemma 4. 2:

$$\int_{-\omega_0}^{1-\omega_0} |F_1(\alpha) \cdot F_2(\alpha)|\, d\alpha = O\left(\frac{N}{\log N}\right).$$

Beweis: Mit der Abkürzung $\pi(N) = \sum_{p \leq N} 1$ gibt die Cauchysche Ungleichung:

$$\int_{-\omega_0}^{1-\omega_0} |F_1(\alpha) \cdot F_2(\alpha)|\, d\alpha \leqq \sqrt{\int |F_1|^2\, d\alpha \cdot \int |F_2|^2\, d\alpha} = \sqrt{\pi\left(\frac{N}{b_1}\right) \cdot \pi\left(\frac{N}{b_2}\right)} = O\left(\frac{N}{\log N}\right).$$

Aus Lemma 4. 1 und 4. 2 folgt sofort

Lemma 4. 3:

$$(4,12)\qquad \Big|\int_{\mathfrak{m}} F(\alpha) \cdot e(-N\alpha)\, d\alpha\Big| = O\left\{N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-A_0 r - \frac{A}{7}(s-2)+s-3}\right\}.$$

Beweis:

$$\Big|\int_{\mathfrak{m}} F(\alpha) \cdot e(-N\alpha)\, d\alpha\Big| \leqq \max_{\alpha \in \mathfrak{m}} |F_3(\alpha) \cdots F_s(\alpha) \cdot F_1'(\alpha) \cdots F_r'(\alpha)| \cdot \int_{-\omega_0}^{1-\omega_0} |F_1 \cdot F_2|\, d\alpha.$$

5. Approximation in den Basisintervallen.

Lemma 5. 1: *Sei* $f(x) = a_0 x^k + a_1 x^{k-1} + \cdots + a_k$ *ein Polynom mit ganzen Koeffizienten vom Grade* $k \geqq 1$. *Sei* $a_0 > 0$. *Wir setzen:*

$$(5,1) = (2,1)\qquad W_{a,q,f} = \sum_{\substack{1 \leq x \leq q \\ (x,q)=1}} e\left(\frac{a}{q} \cdot f(x)\right),$$

$$(5,2)\qquad F_0(\alpha, P) = \sum_{p \leq P} e\big(\alpha \cdot f(p)\big),\quad mit\quad P = \left[\sqrt[k]{\frac{N}{a_0}}\right].$$

Sei

$$(5,3)\quad \alpha \in \mathfrak{M}_{a,q},\ also\ \alpha = \frac{a}{q} + \beta\ mit\ (a,q) = 1,\ |\beta| \leqq \omega_0 = \frac{\log^A N}{N}\ und\ 0 < q \leqq \log^A N.$$

Dann ist mit einer Konstanten $c_1 > 0$

$$(5,4)\quad F_0\left(\frac{a}{q} + \beta, P\right) = \frac{W_{a,q,f}}{\varphi(q)} \cdot \sum_{m=2}^{P} \frac{e(\beta f(m))}{\log m} + O\left(q \cdot N^{\frac{1}{k}} \log^A N \cdot \exp\left(-c_1 \cdot \sqrt{\frac{\log N}{k}}\right)\right).$$

Speziell ist für $f(x) = b \cdot x$, $\alpha \in \mathfrak{M}_{a,q}$; $b > 0$ *ganz:*

$$(5,5)\quad \sum_{p \leq \frac{N}{b}} e(\alpha \cdot b \cdot p) = \frac{D_q(b)}{\varphi(q)} \cdot \sum_{m=2}^{\frac{N}{b}} \cdot \frac{e(b\beta m)}{\log m} + O\left(q \cdot N \cdot \log^A N \cdot \exp\left(-c_1 \cdot \sqrt{\log N}\right)\right).$$

Dabei ist $D_q(b)$ *durch* (2, 2), ω_0 *durch* (4, 6) *gegeben.*

Beweis: Auf Grund des Primzahlsatzes Satz I, 4 gilt für $3 \leqq Q \leqq P$:

$$(5,6)\quad F_0\left(\frac{a}{q}, Q\right) = \left\{ \sum_{\substack{p \leqq Q \\ (p,q)>1}} + \sum_{\substack{p \leqq Q \\ (p,q)=1}} \right\} e\left(\frac{a}{q} \cdot f(p)\right) = O(q) + \sum_{\substack{x=1 \\ (x,q)=1}}^{q} e\left(\frac{a}{q} \cdot f(x)\right) \cdot \pi(Q; q, x)$$

$$= \frac{W_{a,q,f}}{\varphi(q)} \cdot \sum_{m=2}^{Q} \frac{1}{\log m} + O\left(q \cdot P \cdot \exp\left(-c_1 \cdot \sqrt{\frac{\log N}{k}}\right)\right)$$

wegen $|W_{a,q,f}| \leqq q$. Sei

$$(5,7)\qquad g(\beta, f, P) = \sum_{m=2}^{P} \frac{e(\beta f(m))}{\log m}.$$

Nach dem Additionstheorem Satz I, 3 ist

$$g(\beta, f, P) = g(0, f, P) \cdot e(\beta f(P)) - 2\pi i\beta \cdot \int_0^P e(\beta f(z)) \cdot f'(z) \cdot \sum_{m=2}^{z} \frac{1}{\log m}\, dz$$

und

$$F_0\left(\frac{a}{q} + \beta, P\right) = F_0\left(\frac{a}{q}, P\right) \cdot e(\beta f(P)) - 2\pi i\beta \cdot \int_0^P e(\beta f(z)) \cdot f'(z) \cdot \sum_{p=2}^{z} e\left(\frac{a}{q} \cdot f(p)\right) dz.$$

Somit wird unter Benützung von (5, 3) $|\beta| \leqq \omega_0$ und (5, 6):

$$\left|F_0\left(\frac{a}{q} + \beta, P\right) - \frac{W_{a,q,f}}{\varphi(q)} \cdot g(\beta, f, P)\right| = O\left(q \cdot P \cdot \exp\left(-c_1 \sqrt{\frac{\log N}{k}}\right)\right)$$

$$+ 2\pi \cdot |\beta| \cdot \left| \int_0^P e(\beta f(z)) \cdot f'(z) \cdot \left\{ \sum_{p \leqq z} e\left(\frac{a}{q} f(p)\right) - \frac{W_{a,q,f}}{\varphi(q)} \cdot \sum_{m=2}^{z} \frac{1}{\log m} \right\} dz \right|$$

$$= O\left(q \cdot P \cdot \log^A N \cdot \exp\left(-c_1 \cdot \sqrt{\frac{\log N}{k}}\right)\right).$$

Für (5, 5) beachtet man noch, daß nach (2, 7) $D_q(ab) = D_q(b)$ wegen $(a, q) = 1$ ist.

Lemma 5. 2: *Sei* (4, 1) $P_j = \left[\sqrt[k_j]{\frac{N}{a_{0j}}}\right]$ $(j = 1, \ldots, r)$,

$$(5,8)\quad \Sigma_1 = \sum_{\substack{2 \leqq m_\sigma \leqq \frac{N}{b_\sigma},\ (\sigma=1,\ldots,s) \\ 2 \leqq m'_j \leqq P_j\ \ (j=1,\ldots,r)}} \frac{e(\beta \cdot \{b_1 m_1 + \cdots + b_s m_s + f_1(m'_1) + \cdots + f_r(m'_r)\})}{\log m_1 \cdots \log m_s \cdot \log m'_1 \cdots \log m'_r}.$$

Für $\alpha \in \mathfrak{M}_{a,q}$, *also* $\alpha = \frac{a}{q} + \beta$ *mit* $|\beta| \leqq \omega_0$ *ist dann*

$$(5,9)\quad F\left(\frac{a}{q} + \beta\right) = \frac{\prod_{\sigma=1}^{s} D_q(b_\sigma)}{(\varphi(q))^s} \cdot \frac{\prod_{j=1}^{r} W_{a,q,f_j}}{(\varphi(q))^r} \cdot \Sigma_1$$

$$+ O\left(N^{s+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-(s+r)+1} \cdot \log^{2A} N \cdot \exp\left(-c_1 \cdot \sqrt{\frac{\log N}{k^*}}\right)\right)$$

mit $k^* = \max(1, k_1, \ldots, k_r)$. $F(\alpha)$ *ist durch* (4, 4) *gegeben.*

Der *Beweis* folgt unmittelbar aus Lemma 5. 1 unter Beachtung der aus (4, 2) und (4, 3) folgenden trivialen Abschätzungen:

$$|F_\sigma(\alpha)| = O\left(\frac{N}{\log N}\right); \quad |F'_j(\alpha)| = O\left(\frac{N^{\frac{1}{k_j}}}{\log N}\right)$$

Lemma 5. 3: *Der Beitrag $w(a, q)$ eines Basisintervalles zu $r(N)$* (vgl. (4, 8)) *ist:*

$$(5, 10)\quad w(a, q) = w^*(a, q) + O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-(s+r)+1} \cdot (\log N)^{3A} \cdot \exp\left(-c_1 \cdot \sqrt{\frac{\log N}{k^*}}\right)\right)$$

mit

$$(5, 11)\quad w^*(a, q) = (\varphi(q))^{-(r+s)} \cdot \prod_{\sigma=1}^{s} D_q(b_\sigma) \cdot \prod_{j=1}^{r} W_{a,q,f_j} \cdot e\left(-\frac{a}{q} \cdot N\right) \cdot \int_{-\omega_0}^{+\omega_0} \Sigma_1 \cdot e(-\beta N)\, d\beta.$$

Dabei ist D_q durch (2, 3), *$W_{a,q}$ durch* (2, 2) *und Σ_1 durch* (5, 8) *gegeben.*

Beweis: Mit der Integralsubstitution $\beta = \alpha - \frac{a}{q}$ und Lemma 5. 2 erhält man:

$$w(a, q) = \int_{\frac{a}{q}-\omega_0}^{\frac{a}{q}+\omega_0} F(\alpha) \cdot e(-N\alpha)\, d\alpha$$

$$= \frac{\prod_{\sigma} D_q(b_\sigma) \cdot \prod_{j} W_{a,q,f_j}}{(\varphi(q))^{r+s}} \cdot \int_{-\omega_0}^{+\omega_0} \Sigma_1 \cdot e(-N\beta)\, d\beta \cdot e\left(-\frac{a}{q} \cdot N\right)$$

$$+ O\left(N^{s+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-(s+r)+1} \cdot \log^{2A} N \cdot \exp\left(-c_1 \sqrt{\frac{\log N}{k^*}}\right) \cdot \frac{\log^A N}{N}\right).$$

Lemma 5. 4: *Sei $2 \leqq t \leqq s$. $b_1, \ldots, b_t$ seien ganze positive Zahlen mit $(b_1, \ldots, b_t) = 1$. Wir setzen:*

$$(5, 12)\qquad g(\alpha, Q) = \sum_{m=2}^{Q} \frac{e(\alpha m)}{\log m}.$$

Für $0 < |\beta| \leqq (2 \cdot b_1 b_2 \cdots b_t)^{-1}$ ist dann

$$(5, 13)\qquad \left|g\left(b_\tau \beta, \frac{N}{b_\tau}\right)\right| \leqq \min\left(\frac{1}{|b_\tau \beta|}, 2N\right), \qquad (\tau = 1, \ldots, t).$$

Für $(2 \cdot b_1 b_2 \cdots b_t)^{-1} < |\beta| \leqq \frac{1}{2}$ ist

$$(5, 14)\qquad \left|\prod_{\tau=1}^{t} g\left(b_\tau \beta, \frac{N}{b_\tau}\right)\right| < 2^t \cdot N^{t-1} \cdot \log N.$$

Beweis: Es ist nach Vinogradov (28), Chap. I, Lemma 6

$$\left|\sum_{m=2}^{Q} e(\alpha m)\right| \leqq \min\left(\frac{1}{2\,||\alpha||}, Q\right) \quad (Q > 2).$$

Durch Abelsche Summation (Satz I, 2) folgt nun:

$$|g(\alpha, Q)| \leqq \frac{1}{\log Q} \cdot \left|\sum_{m=2}^{Q} e(\alpha m)\right| + \left|\int_{2}^{Q} \sum_{2 \leqq m \leqq z} e(m\alpha) \cdot \frac{dz}{z \cdot (\log z)^2}\right|$$

$$\leqq \frac{1}{\log Q} \cdot \min\left(\frac{1}{2\,||\alpha||}, Q\right) + \min\left(\frac{1}{2\,||\alpha||}, Q\right) \cdot \left(\frac{1}{\log 2} - \frac{1}{\log Q}\right) < \min\left(\frac{1}{||\alpha||}, 2Q\right),$$

woraus (5. 13) unmittelbar folgt.

Um (5, 14) zu beweisen, folgen wir Richert (19), Lemma 12. Zu jedem β aus $\left[(2b_1 \cdots b_t)^{-1}, \frac{1}{2}\right]$ gibt es a und q mit $(a, q) = 1$, $2 \leqq q \leqq \log N$, $1 \leqq a < q$, so daß $\left|\beta - \frac{a}{q}\right| \leqq \frac{1}{q \cdot \log N}$ ist.

Weil N als genügend groß vorausgesetzt ist, und weil $\frac{1}{2} \geqq \beta \geqq (2b_1 \cdots b_t)^{-1}$ ist, so tritt weder die Möglichkeit $a = 0$ noch $q = 1$ bei der Fareyzerlegung des Intervalls $\left[(2b_1 \cdots b_t)^{-1}, \frac{1}{2}\right]$ auf. Somit ist $b_\tau \beta = \frac{a \cdot b_\tau}{q} + \frac{b_\tau \cdot \Theta}{q \cdot \log N}$, $(\tau = 1, \ldots t)$ mit $|\Theta| \leqq 1$. Den Kongruenzwert $a \cdot b_\tau \equiv f_\tau \bmod q$ bezeichnen wir mit f_τ, und es ist o. B. d. A. $0 \leqq f_\tau \leqq q - 1$. Also wird:

$$\| b_\tau \beta \| = \left\| \frac{f_\tau}{q} + \frac{b_\tau \Theta}{q \log N} \right\|.$$

Weil N als genügend groß vorausgesetzt ist, folgt:

$$| b_\tau \Theta \cdot q^{-1} (\log N)^{-1} | \leqq \frac{1}{4q}.$$

Somit gilt, falls $1 \leqq f_\tau \leqq q - 1$ ist:

$$0 < \frac{1}{2q} \leqq \frac{f_\tau}{q} + \frac{b_\tau \Theta}{q \log N} \leqq 1 - \frac{1}{2q} < 1,$$

also

$$\left\| \frac{f_\tau}{q} + \frac{b_\tau \Theta}{q \log N} \right\| \geqq \frac{1}{2q},$$

also

$$\left\| \frac{f_\tau}{q} + \frac{b_\tau \Theta}{q \log N} \right\|^{-1} \leqq 2q \leqq 2 \cdot \log N \text{ für } 1 \leqq f_\tau \leqq q - 1.$$

Ist $f_\tau = 0$, so haben wir

$$\left| g\left(b_\tau \beta, \frac{N}{b_\tau}\right) \right| \leqq \frac{1}{\log 2} \cdot \sum_{m=2}^{N/b_\tau} | e(m b_\tau \beta) | < 2N.$$

$f_\tau = 0$ ist wegen $a \cdot b_\tau \equiv f_\tau \bmod q$ und $(a, q) = 1$ gleichbedeutend mit $q \mid b_\tau$. $1 \leqq f_\tau \leqq q - 1$ ist gleichbedeutend mit $q \nmid b_\tau$ $(\tau = 1, \ldots, t)$.

Weil $(b_1, \ldots, b_t) = 1$ und $q \geqq 2$ ist, so kann q höchstens in $t - 1$ der Zahlen $b_1, \ldots, b_t$ aufgehen, also kann wenigstens ein $g\left(b_\tau \beta, \frac{N}{b_\tau}\right)$ durch $2 \cdot \log N$ abgeschätzt werden, woraus (5, 14) für $(2b_1 \cdots b_t)^{-1} \leqq \beta \leqq \frac{1}{2}$ folgt. Für $-\frac{1}{2} \leqq \beta \leqq -(2b_1 \cdots b_t)^{-1}$ verläuft der Beweis analog.

Lemma 5. 5: Es ist

$$Z = \left| \left\{ \int_{-\frac{1}{2}}^{+\frac{1}{2}} - \int_{-\omega_0}^{+\omega_0} \right\} \Sigma_1 \cdot e(-\beta N)\, d\beta \right| \ll \frac{N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}}}{(\log^A N)}.$$

Beweis: a) Für $r \geqq 1$ ist mit $\omega_0 = \frac{1}{N} \cdot \log^A N$ und $B_s =_{\text{Df.}} (2b_1 \cdots b_s)^{-1}$

$$Z \leqq 2 \cdot \int_{\omega_0}^{\frac{1}{2}} | \Sigma_1 \cdot e(-\beta N) |\, d\beta \leqq 2 \cdot \left\{ \int_{\omega_0}^{B_s} + \int_{B_s}^{\frac{1}{2}} \right\} | \Sigma_1 \cdot e(-\beta N) |\, d\beta$$

$$\leqq 2 \cdot \left\{ \int_{\omega_0}^{B_s} + \int_{B_s}^{\frac{1}{2}} \right\} \left| \prod_{\sigma=1}^{s} g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right) \right| \cdot | \Sigma_2 |\, d\beta = 2 \cdot (J_1 + J_2)$$

mit

$$\Sigma_2 = \sum_{2 \leq m_j' \leq P_j \; (j=1,\ldots,r)} \frac{e(\beta \cdot \{f_1(m_1') + \cdots + f_r(m_r')\})}{\log m_1' \cdots \log m_r'}.$$

Die triviale Abschätzung von Σ_2 gibt:

$$|\Sigma_2| \leqq (\log 2)^{-r} \cdot N^{\frac{1}{k_1} + \cdots + \frac{1}{k_r}}.$$

Nach Lemma 5. 4 (5, 13) mit $t = s$ ist in $[\omega_0, (2b_1 \cdots b_s)^{-1}]$

$$\left| \prod_{\sigma=1}^{s} g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right) \right| \leqq (b_1 \cdots b_s)^{-1} \cdot |\beta|^{-s}$$

und

$$\int_{\omega_0}^{B_s} |\beta|^{-s} \, d\beta = O(N^{s-1} \cdot (\log N)^{-A(s-1)}),$$

also wird:

$$J_1 \ll \frac{N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}}}{(\log N)^{A(s-1)}}.$$

Nach Lemma 5. 4 (5, 14) ist in $\left[(2b_1 \cdots b_s)^{-1}, \frac{1}{2}\right]$ wegen $(b_1, \ldots, b_s) = 1$

$$\left| \prod_{\sigma=1}^{s} g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right) \right| \leqq 2^s \cdot N^{s-1} \cdot \log N,$$

somit wird:

$$J_2 \leqq 2^s \cdot N^{s-1} \log N \int_{B_s}^{\frac{1}{2}} |\Sigma_2| \, d\beta \leqq 2^s \cdot N^{s-1} \log N \cdot \sqrt{\int_0^1 |\Sigma_2|^2 \, d\beta}.$$

Nun ist

$$|\Sigma_2|^2 = \sum_{2 \leq m_j' \leq P_j} \sum_{2 \leq n_j' \leq P_j} \frac{e(\beta\{f_1(m_1') + \cdots + f_r(m_r') - f_1(n_1') - \cdots - f_r(n_r')\})}{\log m_1' \cdots \log m_r' \cdot \log n_1' \cdots \log n_r'}.$$

Beachtet man, daß

$$\int_0^1 e(\beta u) \, d\beta = \begin{cases} 1 & \text{für } u = 0 \\ 0 & \text{für } u \neq 0, \; u \text{ ganz}, \end{cases}$$

ist, so sieht man, daß J_2 durch $(\log 2)^{-2r} \cdot L''$ abgeschätzt werden kann, wobei L'' die Lösungsanzahl der diophantischen Gleichung

$$f_1(m_1') + \cdots + f_r(m_r') = f_1(n_1') + \cdots + f_r(n_r') \qquad (2 \leqq m_j', n_j' \leqq P_j)$$

ist, und diese ist offensichtlich

$$L'' < c_{15} \cdot N^{2\left(\frac{1}{k_1} + \cdots + \frac{1}{k_r}\right) - \frac{1}{k_1}}.$$

Hieraus folgt für $r \geqq 1$:

$$J_2 \ll N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}-\frac{1}{2k_1}} \cdot \log N.$$

b) Für $r = 0$, $s \geqq 3$ ist

$$Z \leqq 2 \cdot \int_{\omega_0}^{B_s} |\Sigma_1 \cdot e(-\beta N)| \, d\beta + 2 \cdot \int_{B_s}^{\frac{1}{2}} \left| \prod_{\sigma=1}^{s} g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right) \right| d\beta = J_1 + J_2.$$

Wie unter a) ist

$$J_1 \ll \frac{N^{s-1}}{(\log N)^{A(s-1)}}.$$

Um J_2 abzuschätzen, zerlegt man das Intervall $\left[B_s, \frac{1}{2}\right]$ in höchstens $(\log N)^2$ Teilintervalle $\mathfrak{i}_{a,q}$: Zu jedem $\beta \in \left[B_s, \frac{1}{2}\right]$ gibt es nämlich ein a und q mit $(a, q) = 1$, $2 \leqq q \leqq \log N$, $1 \leqq a < q$, so daß $\left|\beta - \frac{a}{q}\right| \leqq \frac{1}{q \log N}$ ist (vgl. den Beweis von Lemma 5. 4).

Aus dem Beweis von Lemma 5. 4 (5, 14) geht hervor, daß in jedem dieser Intervalle $\mathfrak{i}_{a,q}$ wenigstens für ein $g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right)$, etwa für $g\left(b_{\sigma_0} \beta, \frac{N}{b_{\sigma_0}}\right)$ gilt:

$$\left|g\left(b_{\sigma_0} \beta, \frac{N}{b_{\sigma_0}}\right)\right| < 2 \cdot \log N,$$

also ist

$$\int_{\mathfrak{i}_{a,q}} \left|\prod_{\sigma=1}^{s} g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right)\right| d\beta \leqq 2 \cdot \log N \cdot \int_{\mathfrak{i}_{a,q}} \left|\prod_{\substack{\sigma=1 \\ \sigma \neq \sigma_0}}^{s} g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right)\right| d\beta$$

$$\leqq 2 \cdot \log N \cdot \sqrt{\int_0^1 \left|\prod_{\substack{\sigma=1 \\ \sigma \neq \sigma_0}}^{s} g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right)\right|^2 d\beta} \leqq 2 \cdot \log N \cdot \sqrt{L'''},$$

wobei L''' die Lösungsanzahl der diophantischen Gleichung

$$\sum_{\substack{\sigma=1 \\ \sigma \neq \sigma_0}}^{s} b_\sigma m_\sigma = \sum_{\substack{\sigma=1 \\ \sigma \neq \sigma_0}}^{s} b_\sigma n_\sigma, \qquad \left(2 \leqq m_\sigma, n_\sigma \leqq \frac{N}{b_\sigma}\right),$$

ist. Wegen

$$L''' = O\left(N^{2s-2-1}\right)$$

folgt

$$\int_{a,q} \left|\prod_{\sigma=1}^{s} g\left(b_\sigma \beta, \frac{N}{b_\sigma}\right)\right| d\beta \ll N^{s-1-\frac{1}{2}} \cdot \log N,$$

und

$$J_2 \ll (\log N)^2 \cdot N^{s-1-\frac{1}{2}} \cdot \log N.$$

Lemma 5. 6:

$$(5, 14) \qquad w(a, q) = \frac{\prod_{\sigma=1}^{s} D_q(b_\sigma) \cdot \prod_{j=1}^{r} W_{a,q,t_j}}{(\varphi(q))^{r+s}} \cdot e\left(-\frac{a}{q} N\right) \cdot \varrho(N)$$

$$+ O\left\{N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot \left((\log N)^{3A+1-(s+r)} \cdot \exp\left(-c_1 \sqrt{\frac{\log N}{k^*}}\right)\right.\right.$$

$$\left.\left. + (\log N)^{-A} \cdot \frac{\prod_{\sigma} D_q(b_\sigma) \cdot \prod_{j} W_{a,q,t_j}}{(\varphi(q))^{r+s}}\right)\right\}.$$

Beweis: Es ist nach (3, 11) und (5, 8)

$$\varrho(N) = \int_{-\frac{1}{2}}^{+\frac{1}{2}} \Sigma_1 \cdot e(-\beta N)\, d\beta.$$

Unter Beachtung von Lemma 5. 3 und 5. 5 folgt hieraus unmittelbar die Behauptung.

Lemma 5. 7: *Der Beitrag W aller Basisintervalle zu $r(N)$ (vgl. (4, 8)) ist:*

$$W = \sum_{1 \leq q \leq \log^A N} \sum_{\substack{0 \leq a \leq q-1 \\ (a,q)=1}} w(a, q) = \mathfrak{S}(N) \cdot \varrho(N)$$
$$+ O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}}\left((\log N)^{-A} + (\log N)^{-\frac{A}{2k^*}-(r+s)}\right)\right).$$

Beweis: Zunächst ist nach (2, 10) $\prod_{\sigma=1}^{s} D_q(b_\sigma) = O(1)$ und nach Lemma 2. 1:

$$\prod_{j=1}^{r} |W_{a,q,l_j}| = O\left(q^{r-\frac{r}{2k}}\right), \qquad k = \max(k_1, \ldots, k_r).$$

Die Aufsummation der Fehlerglieder in Lemma 5. 6 gibt mit $k^* = \max(1, k)$:

$$\sum_{q=1}^{\log^A N} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot \left((\log N)^{3A-(s+r)+1} \cdot \exp\left(-c_1 \cdot \sqrt{\frac{\log N}{k^*}}\right) + (\log N)^{-A} \cdot \frac{\prod_j |W_{a,q,l_j}|}{(\varphi(q))^{r+s}}\right)\right)$$
$$= O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}}\left((\log N)^{5A-(s+r)+1} \cdot \exp\left(-c_1 \cdot \sqrt{\frac{\log N}{k^*}}\right) + (\log N)^{-A} \cdot \sum_{q=1}^{\log^A N} \frac{q^{r-\frac{r}{2k}} \cdot q^{1+s}}{q^{r+s}}\right)\right)$$
$$= O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-A}\right),$$

denn es ist

$$\exp\left(-c_1 \cdot \sqrt{\frac{\log N}{k^*}}\right) = O(\log^{-6A} N).$$

Weiterhin ist nach (2, 3) und (2, 7)

$$\sum_{q=1}^{\log^A N} \sum_{\substack{a=0 \\ (a,q)=1}}^{q-1} \frac{\prod_\sigma D_q(b_\sigma) \cdot \prod_j W_{a,q,l_j}}{(\varphi(q))^{r+s}} \cdot e\left(-\frac{a}{q} N\right) = \sum_{q=1}^{\log^A N} A(N, q).$$

Setzen wir zur Abkürzung $\mathfrak{S}'(N) = \sum_{q=1}^{\log^A N} A(N, q)$, so ist nach (2, 12)

$$|\mathfrak{S}(N) - \mathfrak{S}'(N)| = O\left((\log N)^{-\frac{A}{2k^*}}\right).$$

Wegen (3, 13)

$$\varrho(N) = O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-(r+s)}\right)$$

folgt das Ergebnis.

Hauptsatz: $r(N) = \mathfrak{S}(N) \cdot \varrho(N)$

$$+ O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-(s+r)} \cdot \left\{(\log N)^{s+r-A_0 r-\frac{A}{7}(s-2)+s-3}\right.\right.$$
$$\left.\left. + (\log N)^{-A+(s+r)} + (\log N)^{-\frac{A}{2k^*}}\right\}\right)$$
$$= \mathfrak{S}(N) \cdot \varrho(N) + O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot (\log N)^{-(s+r)} \cdot (\log N)^{-B}\right),$$

wobei

$$B = \min\left\{-2(s+r) + 3 + A_0 r + \frac{A}{7}(s-2);\ A - (s+r);\ \frac{A}{2k^*}\right\}$$

mit

$$A_0 = A \cdot 2^{-2k} \cdot (4k+4)^{-1}, \quad k = \max(k_1, \ldots, k_r), \quad k^* = \max(1, k)$$

ist.

Dies folgt sofort aus Lemma 4. 3 und Lemma 5. 7. Mit Satz II, 3 bzw. II, 3′ und Satz II, 5 (3, 13) und den Voraussetzungen über A folgt der zu Beginn des II. Abschnittes formulierte Hauptsatz.

Wir können nun durch Spezialisierung verschiedene — meist bekannte — Ergebnisse erhalten.

Korollar II, 1: *Jedes hinreichend große ungerade natürliche N ist in der Gestalt $N = p_1 + p_2 + p_3^k$ darstellbar* (Hua (12), v. d. Corput (1) und (3); vgl. auch v. d. Corput (2)).

Spezialfall $k = 1$: *Jedes hinreichend große ungerade N ist in der Gestalt $N = p_1 + p_2 + p_3$ darstellbar* (Vinogradov (24); leicht lesbare Darstellungen bei Estermann (7), S. 52—67 und Prachar (18), s. 177 ff.). *Die Lösungsanzahl $r(N)$ ist*

$$r(N) = \frac{k^2}{k+1} \cdot \mathfrak{S}(N) \cdot \frac{N^{1+\frac{1}{k}}}{(\log N)^3} + O\left(N^{1+\frac{1}{k}} \cdot \log\log N \cdot (\log N)^{-4}\right)$$

mit

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \frac{\mu^2(q)}{\varphi^3(q)} \cdot \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{\substack{x=1 \\ (x,q)=1}}^{q} e\left(\frac{a}{q}(x^k - N)\right).$$

Korollar II, 2: *Jedes hinreichend große natürliche N mit $N \equiv s + a_{01} + \cdots + a_{0r} \bmod 2$ ist in der Gestalt*

$$N = p_1 + \cdots + p_s + a_{01} p_1'^k + \cdots + a_{0r} p_r'^k \quad (k \geqq 2,\ a_{0j} > 0,\ j = 1, \ldots, r)$$

darstellbar, falls $s \geqq 2$ und $r \geqq 1$ oder $s \geqq 3$ ist. Die Lösungszahl $r(N)$ ist:

$$r(N) = \frac{\left(\Gamma\left(\frac{1}{k}\right)\right)^r}{\Gamma\left(s + \frac{r}{k}\right)} \cdot \frac{N^{s-1+\frac{r}{k}}}{(\log N)^{r+s}} \cdot \frac{\mathfrak{S}(N)}{\sqrt[k]{\prod_{j=1}^{r} a_{0j}}} + O\left(\frac{N^{s-1+\frac{r}{k}}}{(\log N)^{r+s}} \cdot \frac{\log\log N}{\log N}\right)$$

mit

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \frac{\mu^s(q)}{(\varphi(q))^{r+s}} \cdot \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \prod_{j=1}^{r} \left(\sum_{\substack{x_j=1 \\ (x_j,q)=1}}^{q} e\left(\frac{a}{q} \cdot a_{0j} x_j^k\right)\right) \cdot e\left(-\frac{a}{q} N\right).$$

Beweis: Auf Grund des Hauptsatzes mit (3, 13) muß nur noch gezeigt werden, daß $\dfrac{1}{(s-1)!} E_r' \cdot k_r = \dfrac{\left(\Gamma\left(\frac{1}{k}\right)\right)^r}{\Gamma\left(s + \frac{r}{k}\right)}$ ist.

Dabei ist nach Satz II, 4:

$$E_r' = \prod_{j=0}^{r-1} E_j^* \quad \text{mit} \quad E_j^* = \frac{1}{k} \cdot \mathrm{B}\left(\frac{1}{k}, s + \frac{j}{k}\right).$$

Also:

$$E_j^* = \frac{1}{k} \cdot \frac{\Gamma\left(\frac{1}{k}\right) \cdot \Gamma\left(s + \frac{j}{k}\right)}{\Gamma\left(s + \frac{j+1}{k}\right)}$$

und

$$E'_r = \frac{1}{k^r} \cdot \left(\Gamma\left(\frac{1}{k}\right)\right)^r \cdot \Gamma(s) \cdot \left(\Gamma\left(s + \frac{r}{k}\right)\right)^{-1} = \frac{1}{k^r} \cdot \left(\Gamma\left(\frac{1}{k}\right)\right)^r \cdot \frac{(s-1)!}{\Gamma\left(s + \frac{r}{k}\right)}.$$

Korollar II, 3: *Sei N hinreichend groß, $s \geqq 3$, $b_\sigma > 0$, ganz, $(\sigma = 1, \ldots, s)$, $N \equiv b_1 + \cdots + b_s \bmod 2$, $(b_1, \ldots, b_s) = 1$ und N zu je $(s-1)$ der $b_\sigma (\sigma = 1, \ldots, s)$ teilerfremd. Dann ist N in der Form*

$$N = b_1 p_1 + \cdots + b_s p_s$$

darstellbar (Richert (19), der jedoch neben $N \equiv b_1 + \cdots + b_s \bmod 2$ und $s \geqq 3$ die stärkere Voraussetzung $(b_i, b_j) = 1$ für $i \neq j$ hat).

Anmerkung: Läßt man statt Primzahlen $p'_1, \ldots, p'_r$ im Hauptsatz natürliche Variable $x_1, \ldots, x_r$ zu, so erhält man für die Darstellungsanzahl $\tilde{r}(N)$ von N in der Gestalt

$$N = p_1 + \cdots + p_s + f_1(x_1) + \cdots + f_r(x_r) \quad \text{(mit den Bezeichnungen (1, 1))},$$

falls $s \geqq 2$ und $r \geqq 1$ oder $s \geqq 3$ ist:

$$\tilde{r}(N) = \tilde{\mathfrak{S}}(N) \cdot \frac{\tilde{L}}{(\log N)^s} + O\left(N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}} \cdot \frac{\log\log N}{(\log N)^{s+1}}\right).$$

Dabei ist:

$$\tilde{L} = \frac{E_r}{(s-1)!} \cdot \frac{1}{a_{01}^{\frac{1}{k_1}} \cdots a_{0r}^{\frac{1}{k_r}}} \cdot N^{s-1+\frac{1}{k_1}+\cdots+\frac{1}{k_r}}.$$

E_r ist aus Satz II, 4 bekannt. Die Singuläre Reihe ist

$$\tilde{\mathfrak{S}}(N) = \sum_{q=1}^{\infty} \frac{\mu^s(q)}{\varphi^s(q)} \cdot q^{-r} \cdot \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \prod_{j=1}^{r} S_{a,q,f_j} \cdot e\left(-\frac{a}{q} N\right),$$

wobei

$$S_{a,q,f_j} = \sum_{x=1}^{q} e\left(\frac{a}{q} \cdot f_j(x)\right)$$

ist. Speziell erhält man für $f_1(x) = \cdots = f_r(x) = x^2$ Teile der Ergebnisse von Halberstam (9) bzw. G. K. Stanley (23) bzw. Zulauf (29): Die Anzahl der Darstellungen von N in der Gestalt

$$N = p_1 + \cdots + p_s + x_1^2 + \cdots + x_r^2,$$

wobei $s \geqq 2$ und $r \geqq 1$ ist, ist:

$$\tilde{r}(N) = \tilde{\mathfrak{S}}(N) \cdot \frac{N^{s-1+\frac{r}{2}}}{(\log N)^s} \cdot 2^{-r} \cdot \frac{\pi^{\frac{r}{2}}}{\Gamma\left(s + \frac{r}{2}\right)} + O\left(\frac{N^{s-1+\frac{r}{2}}}{(\log N)^s} \cdot \frac{\log\log N}{\log N}\right).$$

Für genügend großes N ist $\tilde{r}(N) > 0$.

Für die Darstellungsanzahl von N in der Gestalt

$$N = p_1 + p_2 + x^k \quad (k \text{ ganz}, k > 1)$$

erhält man:

$$\tilde{r}(N) = \tilde{\mathfrak{S}}(N) \cdot \frac{k}{k+1} \cdot \frac{N^{1+\frac{1}{k}}}{\log^2 N} + O\left(N^{1+\frac{1}{k}} \cdot \log^{-2} N \cdot \frac{\log\log N}{\log N}\right)$$

mit

$$\tilde{\mathfrak{S}}(N) = \sum_{q=1}^{\infty} \frac{\mu^2(q)}{\varphi^2(q)} \cdot \frac{1}{q} \cdot \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \sum_{x=1}^{q} e\left(\frac{a}{q} \cdot x^k\right) \cdot e\left(-\frac{a}{q} N\right).$$

Dieses Ergebnis hat ebenfalls Halberstam in (9) bewiesen. Die Darstellbarkeit wurde schon von v. d. Corput (3) untersucht und ist auch in v. d. Corput (2) enthalten.

Literaturverzeichnis.

(1) *J. G. van der Corput*, Sur le théorème de Goldbach-Vinogradov. C. R. Acad. Sci. Paris **205** (1937), 479—481 und 591—592.

(2) *J. G. van der Corput*, Contribution à la théorie additive des nombres I—VI. Akad. Wet. Amsterdam, Proc. **41** (1938), 227—237; 350—361; 442—453; 556—567; Proc. **42** (1939), 2—12, 336—345.

(3) *J. G. van der Corput*, Über Summen von Primzahlen und Primzahlquadraten, Math. Ann. **116** (1939), 1—50.

(4) *H. Davenport*, On Warings Problem for Cubes. Acta math. **71** (1939), 123—143.

(5) *H. Davenport* und *H. Heilbronn*, On Warings Problem: Two Cubes and one Square. Proc. Lond. Math. Soc. (2) **43** (1937), 73—104.

(6) *H. Davenport* und *H. Heilbronn*, Note on a result in the additive theory of numbers. Proc. Lond. Math. Soc. (2) **43** (1937), 142—151.

(7) *T. Estermann*, Introduction to modern prime number theory, Cambridge 1952.

(8) *W. Gröbner* und *N. Hofreiter*, Integraltafeln II, Wien 1950.

(9) *H. Halberstam*, On the representation of large numbers as sums of squares, higher powers and primes, Proc. Lond. Math. Soc. (2) **53** (1951), 363—380.

(10) *H. Halberstam*, Representation of integers as sums of a square of a prime, a cube of a prime and a cube, Proc. Lond. Math. Soc. (2) **52** (1951), 455—466.

(11) *G. H. Hardy* und *E. M. Wright*, An introduction to the theory of numbers, Oxford 1954.

(12) *Loo-Keng Hua*, Some results in the additive prime number theory. Quart. Journ. Oxford **9** (1938), 68—80.

(13) *Loo-Keng Hua*, On the representation of numbers as the sums of the powers of primes. Math. Z. **44** (1939), 335—346.

(14) *Loo-Keng Hua*, The additive prime number theory. Trav. Inst. Math. Stekloff **22** (1947).

(15) *E. Landau*, Vorlesungen über Zahlentheorie, Leipzig 1927.

(16) *E. Landau*, Über einige neuere Fortschritte der additiven Zahlentheorie. Cambridge Tracts **35** (1937).

(17) *K. Prachar*, Über ein Problem vom Goldbach-Waring'schen Typ, I und II. Monatsh. Math. **57** (1953), 66—74 und 113—116.

(18) *K. Prachar*, Primzahlverteilung, Berlin 1957.

(19) *H.-E. Richert*, Aus der additiven Primzahltheorie, J. f. d. reine und angew. Math. (Crelle) **191** (1953), 179—198.

(20) *K. F. Roth*, Proof, that almost all positive integers are sums of a square, a positive cube and a fourth power. Journ. London Math. Soc. **24** (1949), 4—13.

(21) *K. F. Roth*, A problem in additive number theory, Proc. Lond. Math. Soc. (2) **53** (1951), 381—395.

(22) *K. F. Roth*, On Warings problem for cubes, Proc. Lond. Math. Soc. (2) **53** (1951), 268—279.

(23) *G. K. Stanley*, On the representation of a number as the sum of squares and primes, Proc. Lond. Math. Soc. (2) **29** (1929), 122—144.

(24) *I. M. Vinogradov*, Representation of an odd number as a sum of three primes. C. R. Acad. Sci. URSS **15** (1937), 169—172.

(25) *I. M. Vinogradov*, A new estimation of a trigonometric sum, containing primes. Bull. Acad. Sci. URSS, Sér. Math. Nr. **1** (1938), 1—13.

(26) *I. M. Vinogradov*. A new estimation of a certain sum, containing primes. Rec. math. Moskau **44** (1937), 783 bis 791.

(27) *I. M. Vinogradov*, Einige allgemeine Primzahlsätze. Trav. Inst. Math. Tbilissi **3** (1938), 35—67.

(28) *I. M. Vinogradov*, The method of trigonometrical sums in the theory of numbers. Trav. de l'Inst. math. Stekloff **23** (1947), (in Übersetzung bei Interscience Publishers erschienen).

(29) *A. Zulauf*, Darstellung natürlicher Zahlen als Summen von Primzahlen und Quadraten. J. f. d. reine und angew. Math. (Crelle) **192** (1953), 210—229 und **193** (1954), 39—53, 54—64.

Eingegangen 10. Juli 1959.

Über Winkel- und Transitivitätseigenschaften in Kreisebenen[1][2]. I.

Von *Walter Benz* in Mainz.

W. Süß befaßt sich in [15] mit einer axiomatischen Begründung der klassischen Möbius-Geometrie und hierauf fußend mit einer topologischen Kennzeichnung der linearen Abbildungen auf der Kugel[3]. Er geht aus von einer Kugelfläche F, einem System $\mathfrak{k}$ einfach geschlossener Kurven auf F — genannt Kreise — und einer Gruppe T von indikatrixerhaltenden topologischen Selbstabbildungen von F. (Hieraus folgt nach einem Brouwerschen Fixpunktsatz, daß jede Abbildung von T wenigstens einen Fixpunkt besitzt.) Die Gruppe T wird dabei als minimal dreifach transitiv auf den Punkten von F vorausgesetzt; sie soll weiterhin nur Kreisverwandtschaften enthalten und schließlich dem *Axiom der Winkeltreue*[4]) genügen: Haben zwei Kreise $\varkappa$ und $\varkappa'$ einen Punkt s gemein, und liegt der Punkt $a \neq s$ auf $\varkappa'$, so führt jede T-Abbildung, welche $\varkappa$ in sich selbst überführt und dabei die Punkte s und a einzeln festläßt, auch $\varkappa'$ in sich selbst über. — Süss entwickelt eine Theorie der Winkelvergleichung, die er für einen Beweis des Satzes von Miquel benutzt und die überhaupt die wesentliche Grundlage seiner Argumentation ausmacht.

Die vorliegenden Untersuchungen beschäftigen sich mit einem ähnlichen Problemkreis, allerdings auf allgemeinerem geometrischen Fundament: Dies ist bei uns eine Möbiusebene ([5]), gelegentlich eine $[H]$-Ebene (§ 1), d. i. eine (spezielle) Kreisebene, in der nicht notwendig der Berührsatz zu gelten braucht. Die folgenden Resultate werden vorgelegt:

Im § 2 kennzeichnen wir die Existenz einer dreifach transitiven Gruppe T von Kreisverwandtschaften, die dem Axiom von Süss genügt — eine solche Gruppe ist notwendig minimal dreifach transitiv auf den Punkten (vgl. Satz 3. 2) — durch eine Winkelvergleichung (d. i. eine zweistellige Relation auf der Menge aller Kreiswinkel), deren wichtigste Eigenschaft (bis auf Entartungen) lautet:

---

[1]) Die vorliegende — in zwei Teilen veröffentlichte — Arbeit wurde von der naturwissenschaftlichen Fakultät der Johannes Gutenberg-Universität Mainz als Habilitationsschrift angenommen.

[2]) Auszüge der hier mitgeteilten Untersuchungen wurden vorgetragen im Mathematischen Kolloquium der Universität Freiburg (Brsg.) am 22. 2. 1958 und im Mathematischen Kolloquium der Universität Frankfurt a. M. am 10. 7. 1958.

[3]) Hinsichtlich topologischer Kennzeichnungen lediglich der linearen Abbildungen auf der Kugel vgl. man die weitgehenden Untersuchungen von Kérékjarto [11].

[4]) Wir werden dieses Axiom im folgenden stets zitieren als *Axiom von Süss*. Unter dem *Axiom der Winkeltreue* verstehen wir Eigenschaft IV in § 2.

Gegeben seien zweimal je sieben verschiedene Punkte

$$x_1, x_2, \ldots, x_7 \text{ und } y_1, y_2, \ldots, y_7$$

mit

$$x_i \notin \xi \equiv (x_1 x_2 x_3) \text{ und } y_i \notin \eta \equiv (y_1 y_2 y_3) \text{ für } i = 4, 5, 6, 7.$$

Gilt dann

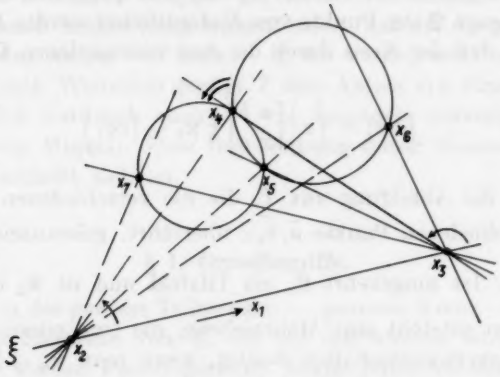
$$(\xi(x_1 x_2 x_i);\, x_2) = (\eta(y_1 y_2 y_i);\, y_2)$$

und

$$(\xi(x_1 x_3 x_i);\, x_3) = (\eta(y_1 y_3 y_i);\, y_3)$$

für $i = 4, 5, 6, 7$, so folgt die Winkelidentität

$$((x_4 x_5 x_6)\,(x_4 x_5 x_7);\, x_4) = ((y_4 y_5 y_6)\,(y_4 y_5 y_7);\, y_4).$$



Bemerkenswert ist, daß diese Winkelvergleichung keineswegs den Peripheriewinkelsatz zur Folge hat, ebenfalls nicht den Satz über den Sehnentangentenwinkel, auch nicht, daß sich zwei Kreise α, β mit $|\alpha \frown \beta| = 2$ unter paarweise gleichen Winkeln schneiden. Jede dieser Eigenschaften erzwingt nämlich die Kommutativität der Winkelgruppe $\mathfrak{W}$, zu der sich die Menge der Klassen gleicher Winkel zusammenfassen läßt (§ 3, Satz 3. 3); wir geben indes ein Beispiel einer Möbiusebene mit Winkelvergleichung der genannten Art, in der $\mathfrak{W}$ die symmetrische Gruppe $\mathfrak{S}_3$ ist (Satz 3. 5ff.). Damit ist die von Smid [14], § 25, in spezielle Möbiusebenen eingeführte Winkelvergleichung wesentlich verallgemeinert: Die von Smid betrachtete Winkelvergleichung (die sich auf alle die von v. d. Waerden und Smid in [17] begründeten Geometrien ausdehnen läßt (s. [4], Sätze 4 bis 8 in Verbindung mit Satz 20)) genügt stets dem Peripheriewinkelsatz und dem Satz über den Sehnentangentenwinkel. Die in den genannten Fällen ebenfalls erfüllte Eigenschaft $(\alpha\beta;\, p) = (\beta\alpha;\, q)$ für $\alpha \frown \beta = \{p, q\}$, $p \neq q$, (s. [4], Satz 9 in Verbindung mit Satz 6), die bei uns nicht notwendig gilt, reduziert sich im Vorliegenden auf den folgenden Sachverhalt (Satz 3. 6): Es existiert ein involutorischer Antiautomorphismus $\varphi \to \bar{\varphi}$ von $\mathfrak{W}$ auf sich derart, daß aus $(\alpha\beta;\, p) = \varphi$ stets $(\beta\alpha;\, q) = \bar{\varphi}$ folgt für verschiedene Kreise α, β, die sich in verschiedenen Punkten p, q schneiden. — Daß der Antiautomorphismus $\varphi \to \bar{\varphi}$ involutorisch ist, kann man sich zur Verpflanzung eines vorgegebenen Winkels in irgendeinen vorgegebenen Punkt zunutze machen (§ 3).

In Teil II dieser Arbeit studieren wir in § 4 Möbiusebenen, die eine minimal dreifach transitive Gruppe T von Kreisverwandtschaften besitzen. Tits kennzeichnet in [16], S. 206ff., minimal dreifach transitive Substitutionsgruppen auf einer strukturlosen Menge E durch eine (mit zwei Kompositionen versehene) algebraische Struktur, die wir *Titsfeld* nennen (s. § 4). Jeder kommutative Körper ist Titsfeld; es gibt eigentliche vollständige Fastkörper (s. Zassenhaus [19], Tits [16]), die ebenfalls Titsfelder sind [5]). — Wir führen den Begriff der *quadratischen Erweiterung* $\mathfrak{K}_2$ *eines Titsfeldes* $\mathfrak{K}_1$ ein (vgl. § 4; hier sei nur die wichtigste — der Definition einer quadratischen Erweiterung zugrundeliegende — Forderung genannt: Zu je zwei Elementen $z, k \in \mathfrak{K}_2 - \mathfrak{K}_1$ gibt es Elemente α, β aus $\mathfrak{K}_1$ mit $z = (\alpha + k)\,\beta$), wir führen ferner den Begriff des Doppelverhältnisses ein als einer jedem geordneten Punktequadrupel a, b, c, d (bestehend aus mindestens drei verschiedenen Punkten) zugewiesenen T-Invarianten $\begin{bmatrix} a & b \\ d & c \end{bmatrix} \in \mathfrak{K}_2 \cup \{\infty\}$; dabei ist ∞ ein Symbol, mit dem in bestimmter Weise gerechnet wird. Dann zeigen wir: Gegeben sei eine Möbiusebene Σ und eine minimal dreifach transitive Gruppe T von Kreisverwandtschaften von Σ. Dann gibt es ein Titsfeld $\mathfrak{K}_1$ und eine quadratische Erweiterung $\mathfrak{K}_2$ von $\mathfrak{K}_1$ derart, daß die Menge $\mathfrak{P}$ der Punkte von Σ identifiziert werden kann mit $\mathfrak{K}_2$ vermehrt um ein Element ∞, daß der Kreis durch die drei verschiedenen Punkte a, b, c gegeben ist durch

$$\text{(D)} \qquad (abc) = \left\{ x \,\middle|\, \begin{bmatrix} a & b \\ x & c \end{bmatrix} \in \mathfrak{K}_1 \cup \{\infty\} \right\}$$

und daß schließlich die Abbildung aus T, die die verschiedenen Punkte a, b, c nacheinander in die verschiedenen Punkte $\bar{a}, \bar{b}, \bar{c}$ überführt, gekennzeichnet ist durch $x \to \bar{x}$ mit $\begin{bmatrix} a & b \\ x & c \end{bmatrix} = \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{x} & \bar{c} \end{bmatrix}$ [6]). Ist umgekehrt $\mathfrak{K}_1$ ein Titsfeld und ist $\mathfrak{K}_2$ eine quadratische Erweiterung von $\mathfrak{K}_1$, so entsteht eine Möbiusebene, die eine minimal dreifach transitive Gruppe T von Kreisverwandtschaften besitzt, wenn man $\mathfrak{K}_2 \cup \{\infty\}$ als Punktmenge definiert und die Kreise vermittels (D) einführt. Dabei ist

$$\begin{bmatrix} a & b \\ d & c \end{bmatrix} = \begin{cases} (c-b)^{-1}(d-b) & \\ \dfrac{1}{[(c-a)' - (b-a)']}\,[(d-a)' - (b-a)'] & \text{für} \quad a \neq \infty, \end{cases} \qquad a = \infty$$

wo $a \to a'$ ein spezieller involutorischer Automorphismus der (s. § 4) multiplikativen Gruppe von $\mathfrak{K}_2$ ist.

Im § 5 untersuchen wir Möbiusebenen, die eine dreifach transitive Gruppe T von Kreisverwandtschaften besitzen, die dem Axiom von Süss genügt. Es handelt sich also genau um die Möbiusebenen, die im § 2 durch eine Winkelvergleichung charakterisiert werden. Wir zeigen (Satz 5. 1), daß das Axiom von Süss gekennzeichnet ist durch die Forderung, daß die multiplikative Gruppe $\mathfrak{K}_1^*$ von $\mathfrak{K}_1$ Normalteiler der multiplikativen Gruppe $\mathfrak{K}_2^*$ von $\mathfrak{K}_2$ ist. — In Satz 5. 1 wird weiterhin gezeigt, daß die Winkelgruppe $\mathfrak{W}$ isomorph zur Faktorgruppe $\mathfrak{K}_2^*/\mathfrak{K}_1^*$ ist und die Winkelvergleichung in üblicher Weise durch Doppelverhältnisse induziert wird.

---

[5]) Alle minimal dreifach transitiven Substitutionsgruppen auf endlichen Mengen gibt Zassenhaus schon 1936 an [18]. — Petkantschin untersucht auf beliebigen Mengen minimal dreifach transitive Substitutionsgruppen mit (im wesentlichen) der weiteren Forderung: Zu vier verschiedenen Elementen a, b, c, d gibt es eine Substitution der Gruppe, die a mit b und die c mit d vertauscht (s. [13]).

[6]) In der Bezeichnung von [4] liegt ein $\alpha\beta\gamma$-Quaternar vor.

Eine gewisse Endstufe nehmen die Möbiusebenen über einem euklidischen Körper ein (vgl. § 6) [7]. Diese Möbiusebenen, wir nennen sie euklidische Möbiusebenen, gestatten bezüglich einer ausgezeichneten affinen Ebene einen Entfernungsbegriff mit weitgehend gewohnten Eigenschaften (s. § 6); z. B. gilt gegenüber diesem Entfernungsbegriff der Sekantentangentensatz. Im § 6 kennzeichnen wir die euklidischen Möbiusebenen: Süss verfügt auf Grund eines Brouwerschen Fixpunktsatzes — wie schon früher gesagt — über die Tatsache, daß jede Abbildung von T wenigstens einen Fixpunkt besitzt. Diese Eigenschaft gilt nicht in allen in § 2 betrachteten Geometrien. Wir zeigen nun: Sei Σ eine Möbiusebene. Dann sind folgende Aussagen äquivalent: (1) Σ gestattet eine minimal dreifach transitive Gruppe T von Kreisverwandtschaften so, daß jede Abbildung τ von T wenigstens einen Fixpunkt besitzt. (2) Σ ist euklidisch.

Im § 7 verzichten wir auf die Gültigkeit des Berührsatzes in der jeweils zugrundeliegenden geometrischen Struktur. Wir zeigen den Satz: Sei Σ eine Kreisebene, in der durch drei verschiedene Punkte genau ein Kreis geht, in der jeder Kreis wenigstens drei verschiedene Punkte besitzt und in der es wenigstens einen Kreis gibt. Gestattet dann Σ eine minimal dreifach transitive Gruppe von Kreisverwandtschaften, von denen jede wenigstens einen Fixpunkt besitzt (man erkennt sofort, daß die Ausgangslage von Süss — schon diejenige *ohne* das Axiom von Süss — in der vorliegenden enthalten ist), so gilt in Σ der Satz von Miquel. Weiterhin genügt T dem Axiom von Süss (es ist also bei Süss entbehrlich; entbehrlich natürlich auch — was besonders hervorgehoben sei — zum Beweise des Satzes von Miquel). Eine Beschreibung dieser Geometrien mit Hilfe von Doppelverhältnissen schließt sich an.

§ 1. Grundbegriffe.

Eine Menge $\mathfrak{P}$, in der gewisse Teilmengen — genannt *Kreise* — ausgezeichnet sind heiße *Kreisebene*. Die Elemente von $\mathfrak{P}$, die wir mit kleinen lateinischen Buchstaben $a, b, c, \ldots$ bezeichnen, werden *Punkte* genannt. Kreise geben wir durch kleine griechische Buchstaben $\alpha, \ldots, \xi$ wieder.

Die Kreise α, β heißen *gleich* bzw. *verschieden*, wenn die Teilmengen α, β von $\mathfrak{P}$ gleich bzw. verschieden sind. Der Kreis α *berührt* den Kreis β in p, wenn α und β verschiedene Kreise sind und $\alpha \cap \beta = \{p\}$ ist. Wir schreiben dann auch $\alpha \cap \beta = p$.

Statt $p \in \alpha$ benutzen wir die üblichen Redewendungen: *Der Kreis α geht durch den Punkt p, der Kreis α enthält den Punkt p, der Punkt p liegt auf dem Kreis α* usw. — Die Punktmenge $p, q, r, \ldots$ heißt *konzyklisch*, wenn sie insgesamt einem Kreise $\varkappa$ angehört.

Unter einer *Kreisverwandtschaft* τ einer Kreisebene Σ verstehen wir einen Automorphismus der Struktur $(\mathfrak{P}; \alpha, \beta, \ldots)$, d. h. eine eineindeutige Abbildung $p \to p^\tau$ der Menge der Punkte p von Σ auf sich, die konzyklische Punktmengen in konzyklische und nicht konzyklische Punktmengen in nicht konzyklische überführt. Hintereinanderschaltung zweier Kreisverwandtschaften τ_1, τ_2, $p \to p^{\tau_1 \tau_2}$, ergibt wieder eine Kreisverwandtschaft. Die Menge der Kreisverwandtschaften einer nichtleeren Kreisebene Σ, in der es wenigstens einen Kreis gibt, bildet eine Gruppe $M(\Sigma)$, die wir die *Möbiusgruppe* von Σ nennen. Kreisverwandtschaften bezeichnen wir i. a. durch $\varrho, \sigma, \tau, \upsilon$. Die identische

[7] Über die Rolle der euklidischen Körper in der Geometrie vgl. man Baer [2] und [3], S. 144, Hoffman [10]. Die von Ewald [8] begründeten Möbius-Geometrien sind, wie in [6] gezeigt ist, genau die euklidischen Möbiusebenen.

Kreisverwandtschaft wird durch v (oder 1) bezeichnet. Statt $a^\tau = a'$, $b^\tau = b'$, ... schreiben wir auch $(a, b, \ldots)^\tau = (a', b', \ldots)$. Den Bildkreis des Kreises α gegenüber τ bezeichnen wir gelegentlich durch α^τ. Kombinationen $\alpha^\tau = \beta$, $p^\tau = q, \ldots$ kürzen wir ab durch $(\alpha, p, \ldots)^\tau = (\beta, q, \ldots)$. Bei dieser Bezeichnung kommt es also auf die Reihenfolge der Elemente $\alpha, p, \ldots$ bzw. $\beta, q, \ldots$ an.

Unter einer $[H]$-*Ebene*, $[H]$-*Kreisebene*, verstehen wir eine Kreisebene Σ mit den Eigenschaften:

(H 1) *Durch drei verschiedene Punkte geht genau ein Kreis.*

(H 2) *Jeder Kreis enthält wenigstens drei verschiedene Punkte. Es gibt wenigstens einen Kreis.*

Wegen (H 1) können wir einen Kreis durch drei verschiedene seiner Punkte kennzeichnen. Sind also a, b, c verschiedene Punkte des Kreises $\varkappa$, so schreiben wir auch $(abc) = \varkappa$. Ist τ eine Kreisverwandtschaft, so bezeichnen wir den Bildkreis von (abc) gegenüber τ durch $(abc)^\tau$. Sind also p, q, r irgend drei verschiedene Punkte des Bildkreises $(abc)^\tau$, so ist $(abc)^\tau = (pqr)$. Diese Schreibweise ist zu unterscheiden von $(a, b, c)^\tau = (p, q, r)$, die ja $a^\tau = p$, $b^\tau = q$, $c^\tau = r$ besagt.

Vorgelegt sei eine $[H]$-Kreisebene. Dann wollen wir das geordnete Kreispaar zweier sich mindestens in einem Punkt schneidender Kreise α, β und einen Schnittpunkt s derselben einen *Winkel*, $(\alpha\beta; s)$, nennen. Ist $t \in \alpha \cap \beta$ und $t \neq s$, so ist der Winkel $(\alpha\beta; t)$ von $(\alpha\beta; s)$ zu unterscheiden. Weiterhin zu unterscheiden von den bisher angeschriebenen Winkeln ist $(\beta\alpha; s)$ und entsprechend $(\beta\alpha; t)$. Sind α, β Kreise und ist s ein Punkt, so wird das Symbol $(\alpha\beta; s)$ nur verwendet, wenn $s \in \alpha \cap \beta$ ist.

Eine zweistellige Relation auf der Menge aller Winkel einer $[H]$-Ebene Σ, hier „=" geschrieben, heiße eine *Winkelvergleichung „über"* (*„auf"*, *„in"*) Σ.

Mit den im Vorstehenden eingeführten Winkeln sind im klassischen Falle die orientierten Kreiswinkel gemeint: Man versieht also eine Kugel mit einer Indikatrix und nimmt für $(\alpha\beta; s)$ den der Größe nach eindeutig bestimmten Winkel modulo π, der in s längs der durch die Indikatrix gegebenen Orientierung vom Kreis α zum Kreis β führt.

Eine Kreisebene heißt *Möbiusebene* (s. [5]), wenn gilt:

(1) *Durch drei verschiedene Punkte geht mindestens ein Kreis. Sind α, β, γ verschiedene Kreise mit $|\alpha \cap \beta \cap \gamma| \geqq 2$, so gilt $\alpha \cap \beta = \beta \cap \gamma = \gamma \cap \alpha$.*

(2) *Zu einem Kreis $\varkappa$, einem Punkt $p \in \varkappa$ und einem Punkt $q \notin \varkappa$ gibt es genau einen Kreis $\lambda \ni p, q$ mit $\lambda \cap \varkappa = p$.*

(3) *Jeder Kreis besitzt wenigstens einen Punkt. Es gibt vier verschiedene Punkte, die nicht gemeinsam einem Kreise angehören.*

In einer Möbiusebene besitzt jeder Kreis wenigstens drei verschiedene Punkte (s. [5]).

Echt stärkere Möbiusebenen sind die Kreisebenen, die den Eigenschaften (2), (3) genügen und statt (1) der Eigenschaft

(1′) *Durch drei verschiedene Punkte geht genau ein Kreis.*

Wir nennen eine solche Möbiusebene *„Möbiusebene im engeren Sinne"*, in Zeichen $[M]$-*Ebene* (s. hierzu Smid [14]).

Sei p ein Punkt einer Möbiusebene. Dann verstehen wir unter einem *Berührbüschel* oder einem *Kontaktelement* (*mit Grundpunkt p*) eine maximale Menge sich paarweise in p berührender Kreise[7′]). Ist ein Kreis α eines Berührbüschels gegeben, so bekommt man alle

[7′]) Diese Definition verdanke ich Herrn Professor Baer. — Die Bezeichnung „Kontaktelement" benutzt Smid in [14].

weiteren Kreise des Berührbüschels als die Kreise, die α in p berühren. Da ein Berührbüschel durch einen ihm angehörenden Kreis α und den Grundpunkt p eindeutig bestimmt ist, so läßt es sich auch durch α_p bezeichnen. (α_p ist gelegentlich zu identifizieren mit der Menge der ihm angehörenden Kreise.) Ist $\beta \in \alpha_p$, so hat man $\alpha \in \beta_p$. Ist $\beta \in \alpha_p$ und $\gamma \in \beta_p$, so gilt $\alpha \in \gamma_p$. Statt „*Berührbüschel mit Grundpunkt p*" wird verschiedentlich gesagt „*Berührbüschel durch (in) p*" oder „*Kontaktelement in p*".

§ 2. Eine gruppentheoretisch-geometrische Kennzeichnung einer Winkelvergleichung in $[M]$-Ebenen.

Gegeben sei eine $[M]$-Ebene Σ, in der die Winkel in einer Beziehung „gleich", „$=$", stehen. Es sollen die folgenden Axiome (I), (II), (III), (IV) gelten:

(I) *Sind α, β Kreise durch einen Punkt p, so gilt $(\alpha\beta;\, p) = (\alpha\beta;\, p)$. Sind weiter γ, δ Kreise durch q und ε, ζ Kreise durch r und ist $(\alpha\beta;\, p) = (\gamma\delta;\, q)$, $(\alpha\beta;\, p) = (\varepsilon\zeta;\, r)$, so folgt $(\gamma\delta;\, q) = (\varepsilon\zeta;\, r)$.*

(II) *Sind α, β Kreise und sind p, q Punkte mit $p \in \alpha$, $q \in \beta$, so gilt $(\alpha\alpha;\, p) = (\beta\beta;\, q)$.*

(III) **a)** *Sind α, β Kreise durch einen Punkt p, so gilt $(\alpha\beta;\, p) = (\alpha\xi;\, p)$ genau dann wenn $\xi \in \beta_p$ ist.*

b) *Ist γ ein weiterer Kreis durch den weiteren Punkt q, so gibt es wenigstens einen Kreis $\lambda \ni q$ mit $(\alpha\beta;\, p) = (\gamma\lambda;\, q)$.*

(IV) *Es seien p, q, r verschiedene Punkte und ebenso $p'(= p), q', r'$. Sind dann x_1, x_2, x_3, x_4 und x_1', x_2', x_3', x_4' je vier unter sich verschiedene Punkte mit*

(a) $x_i \notin (pqr) - \{p, q, r\}$, $x_i' \notin (p'\,q'\,r') - \{p', q', r'\}$ *für* $i = 1, 2, 3, 4$,

(b) *für* $x_i =$ *resp.* p, q, r *ist* $x_i' =$ *resp.* p', q', r',

(c) *im Falle* $x_i \notin \{p, q, r\}$ *ist* $x_i' \notin \{p', q', r'\}$ *und weiter*

$$((pqr)\,(pqx_i);\, q) = ((p'q'r')\,(p'q'x_i');\, q'),$$
$$((prq)\,(prx_i);\, r) = ((p'r'q')\,(p'r'x_i');\, r'),$$

so gilt die Winkelidentität

$$((x_1x_2x_3)\,(x_1x_2x_4);\, x_1) = ((x_1'x_2'x_3')\,(x_1'x_2'x_4');\, x_1')\ ^{8)}.$$

Aus (I) folgt, daß sich die Menge aller Winkel von Σ in fremde Klassen gleicher Winkel zerlegen läßt. Diese Klassen bezeichnen wir mit $\varphi, \varphi_1, \ldots \chi, \ldots, \psi, \ldots$. Ist $(\alpha\beta;\, p) \in \varphi$, so schreiben wir $(\alpha\beta;\, p) = \varphi$ oder $\varphi = (\alpha\beta;\, p)$ und nennen φ die „*Maßzahl*" oder die „*Größe*" des Winkels $(\alpha\beta;\, p)$. Die Klassen φ werden auch *freie Winkel* genannt.

Hilfssatz 2. 1. *Sind α, β Kreise durch einen Punkt p, ist γ ein Kreis durch einen Punkt q, dann bilden die Lösungen λ von $(\alpha\beta;\, p) = (\gamma\lambda;\, q)$ genau ein Berührbüschel durch q. Ist q' ein von q verschiedener Punkt, dann gibt es genau einen Kreis $\bar{\lambda} \ni q, q'$ mit $(\alpha\beta;\, p) = (\gamma\bar{\lambda};\, q)$.*

Beweis. Sind λ^1, λ^2 Lösungen λ von $(\alpha\beta;\, p) = (\gamma\lambda;\, q)$, so folgt $(\gamma\lambda^1;\, q) = (\gamma\lambda^2;\, q)$ nach Axiom (I), was $\lambda^2 \in \lambda_q^1$ nach (III) ergibt. Alle Lösungen λ' sind also in λ_q enthalten, wenn λ irgendeine beliebige Lösung darstellt. Ist umgekehrt λ^0 ein Kreis aus λ_q, so gilt $(\gamma\lambda;\, q) = (\gamma\lambda^0;\, q)$ nach (III), d. h. $(\alpha\beta;\, p) = (\gamma\lambda;\, q) = (\gamma\lambda^0;\, q)$; λ^0 ist also Lösung. Schließlich beachte man noch, daß es genau einen Kreis $\bar{\lambda}$ gibt mit $q' \in \bar{\lambda}_q \in \lambda_q$ für $q' \neq q$.

Hilfssatz 2. 2. *Sind α, β Kreise durch den Punkt p und γ, δ Kreise durch den Punkt q mit $(\alpha\beta;\, p) = (\gamma\delta;\, q)$, so folgt aus $\beta \in \alpha_p$ auch $\delta \in \gamma_q$.*

---

[8]) Der Fall $p' \neq p$ kann erschlossen werden.

Beweis. Wegen $\beta \in \alpha_p$ ist nach den Axiomen (III) und (II)

$$(\alpha\beta;\, p) = (\alpha\alpha;\, p) = (\gamma\gamma;\, q), \text{ d. h. } (\gamma\delta;\, q) = (\gamma\gamma;\, q),$$

also $\delta \in \gamma_q$ nach (III).

Mit Hilfssatz 2. 2 ergibt sich

Hilfssatz 2. 3. *Ein spezieller freier Winkel wird gebildet genau von allen Winkeln* $(\alpha\beta;\, p)$, α, β, p *bis auf* $\beta \in \alpha_p$ *beliebig. Dieser freie Winkel wird auch „Nullwinkel", in Zeichen* 0, *genannt.*

Beweis. Ist $(\alpha\beta;\, p) = (\gamma\delta;\, q)$ mit $\beta \in \alpha_p$, so folgt also $\delta \in \gamma_q$. Seien umgekehrt α, β Kreise durch den Punkt p mit $\beta \in \alpha_p$ und γ, δ Kreise durch den Punkt q mit $\delta \in \gamma_q$. Dann ist nach (III) und (II)

$$(\alpha\beta;\, p) = (\alpha\alpha;\, p) = (\gamma\gamma;\, q) = (\gamma\delta;\, q).$$

Mit $T(\Sigma)$ bezeichnen wir die Gruppe derjenigen Kreisverwandtschaften τ, die jeden freien Winkel invariant lassen, für die also stets $(\alpha\beta;\, p) = (\alpha^\tau\beta^\tau;\, p^\tau)$ folgt für Kreise α, β durch einen Punkt p. Wir nennen weiterhin genau diese Elemente der Möbiusgruppe *kreiswinkeltreu.* Die Identität von $T(\Sigma)$ werde mit v bezeichnet.

Dann beweisen wir den für das Folgende wichtigen

Satz 2. 1. *Sind* α, β *Kreise durch den Punkt* p *und ist* τ *eine Abbildung aus* $T(\Sigma)$ *mit* $(\alpha, p)^\tau = (\alpha, p)$, *so ist* $\beta^\tau \in \beta_p$.

Beweis[9]. Aus $(\alpha\beta;\, p) = (\alpha^\tau\beta^\tau;\, p^\tau) \equiv (\alpha\beta^\tau;\, p)$ folgt $\beta^\tau \in \beta_p$ nach Axiom (IIIa).

Über den Zusammenhang der in Satz 2. 1 ausgesprochenen Eigenschaft der Gruppe $T(\Sigma)$ mit dem Axiom von Süss gilt

Satz 2. 2. *Ist* Σ *eine* $[M]$*-Ebene und ist* $\widetilde{T}(\Sigma)$ *irgend eine Gruppe von Kreisverwandtschaften, die der Eigenschaft von Satz* 2. 1 *genügt, so gilt für* $\widetilde{T}(\Sigma)$ *das Axiom von Süss: Haben zwei Kreise* $\varkappa$ *und* $\varkappa'$ *einen Punkt* s *gemein, und liegt der Punkt* $a (\neq s)$ *auf* $\varkappa'$, *so führt jede* $\widetilde{T}(\Sigma)$*-Abbildung* τ, *welche* $\varkappa$ *in sich selbst überführt und dabei die Punkte* s *und* a *einzeln festläßt, auch* $\varkappa'$ *in sich selbst über.*

Beweis. Aus $\varkappa, \varkappa' \ni s$ und $(\varkappa, s)^\tau = (\varkappa, s)$ mit $\tau \in \widetilde{T}(\Sigma)$ folgt $\varkappa'^\tau \in \varkappa'_s$ nach Voraussetzung über $\widetilde{T}(\Sigma)$. Da $\{a^\tau = a,\ s^\tau = s\} < \varkappa'^\tau \cap \varkappa'$ ist, hat man also $\varkappa'^\tau = \varkappa'$.

Satz 2. 3. *Sind* a, b, c *verschiedene Punkte und ebenso* a', b', c', *so gibt es höchstens eine Kreisverwandtschaft* $\tau \in T(\Sigma)$ *mit* $(a, b, c)^\tau = (a', b', c')$.

Beweis. Angenommen, es gäbe verschiedene Abbildungen $\tau_1, \tau_2 \in T(\Sigma)$ mit $(a, b, c)^{\tau_i} = (a', b', c')$, $i = 1, 2$. Es ist dann $(a, b, c)^\tau = (a, b, c)$, $\tau \equiv \tau_1\tau_2^{-1} \in T(\Sigma)$; wir zeigen, daß τ die Identität v und also doch $\tau_1 = \tau_2$ sein müßte. Sei x ein nicht auf (abc) gelegener Punkt. Wegen $\tau \in T(\Sigma)$ folgt

$$\big((abc)\,(abx);\, b\big) = \big((abc)\,(abx^\tau);\, b\big) \text{ und } \big((acb)\,(acx);\, c\big) = \big((acb)\,(acx^\tau);\, c\big).$$

Nach Axiom (IIIa) gilt nun $(abx^\tau) = (abx)$ und $(acx^\tau) = (acx)$. Man hat also $x^\tau \in (abx)$ und $x^\tau \in (acx)$. Da das Punktequadrupel a, b, c, x nicht konzyklisch ist, gilt $x^\tau \in (abx) \cap (acx) = \{a, x\}$ und damit $x^\tau = x$. — Sei x ein auf (abc) gelegener Punkt. Führt man nun die vorangegangene Betrachtung für Punkte a, b, d mit $d \notin (abc)$ (es ist ja dann $d^\tau = d$) anstelle von a, b, c durch, so erkennt man wegen $x \notin (abd)$ wiederum $x^\tau = x$. Damit ist τ tatsächlich die Identität.

---

[9]) Zum Beweis für die Sätze 2. 1, 2. 3 werden lediglich die Axiome (I) und (IIIa) benutzt.

Hilfssatz 2. 4. *Es seien α, β verschiedene Kreise durch die verschiedenen Punkte p, q und α', β' verschiedene Kreise durch die verschiedenen Punkte p, q' mit $(\alpha\beta;\, q) = (\alpha'\beta';\, q')$. Es seien fernerhin a, a' vorgegebene Punkte mit $a \in \alpha - \beta$, $a' \in \alpha' - \beta'$. Dann gibt es Punkte $b \in \beta - \alpha$, $b' \in \beta' - \alpha'$ mit $\big(\alpha(abp);\, a\big) = \big(\alpha'(a'b'p);\, a'\big)$.*

Beweis. Es sei ε der durch $a \in \varepsilon \in \beta_p$ bestimmte Kreis und entsprechend ε' der durch $a' \in \varepsilon' \in \beta'_p$ eindeutig festgelegte Kreis. Dann unterscheiden wir zwei Fälle (man beachte dabei $|\lambda| = |\mu|$ für zwei beliebige Kreise λ, μ, wobei etwa $|\lambda|$ die Mächtigkeit der Menge $\lambda < \mathfrak{P}$ bedeutet):

1) *Jeder Kreis enthält wenigstens vier verschiedene Punkte.*

In diesem Falle gibt es nach (III a) wenigstens drei untereinander und von 0 verschiedene freie Winkel $\varphi_1, \varphi_2, \varphi_3$. Es gibt dann also weiter einen unter diesen freien Winkeln, etwa φ_{i_0}, mit $\varphi_{i_0} \not\ni (\alpha\varepsilon;\, a)$, $(\alpha'\varepsilon';\, a')$. Nun seien γ, γ' die durch

$$\gamma \ni a, p; \quad \gamma' \ni a', p; \quad \varphi_{i_0} \ni (\alpha\gamma;\, a); \quad \varphi_{i_0} \ni (\alpha'\gamma';\, a')$$

nach Hilfssatz 2. 1 eindeutig bestimmten Kreise. Sicherlich ist $\gamma \neq \varepsilon$ und $\gamma' \neq \varepsilon'$. Es ist auch $\gamma \neq \alpha$ und $\gamma' \neq \alpha'$. Damit schneidet γ den Kreis β neben p noch in einem Punkt $b \in \beta - \alpha$; entsprechend ist $\gamma' \cap \beta' = \{p, b'\}$, $b' \neq p$. Wegen $(\alpha\gamma;\, a) = (\alpha'\gamma';\, a')$ und $\gamma = (abp)$, $\gamma' = (a'b'p)$ ist die Behauptung für den Fall 1) bewiesen.

2) *Jeder Kreis enthält genau drei verschiedene Punkte.*

Dann liegt die eindeutig bestimmte Möbiusebene mit insgesamt fünf verschiedenen Punkten und zehn verschiedenen Kreisen vor. Es gibt dann genau drei verschiedene freie Winkel, den Nullwinkel eingeschlossen. Wir behaupten zunächst: Es gilt $(\alpha\beta;\, q) \neq \big(\alpha(abp);\, a\big)$, wenn b der eindeutig bestimmte Punkt mit $b \in \beta - \alpha$ ist. Wäre doch $(\alpha\beta;\, q) = \big(\alpha(abp);\, a\big)$, dann wenden wir Axiom (IV) an. Wir setzen $x_1 = p$, $x_2 = q$, $x_3 = a$, $x_4 = b$ und $x'_1 = p$, $x'_2 = a$, $x'_3 = q$, $x'_4 = b$, wobei $p, q, r \equiv a$ und $p' = p$, $q' = a$, $r' = q$ zugrunde gelegt ist (der jetzt eingeführte Punkt q' ist nicht mit dem bisherigen Punkt q' zu verwechseln). Axiom (IV) ergibt

$$(\alpha\beta;\, p) = \big((x_1x_2x_3)\,(x_1x_2x_4);\, x_1\big) = \big((x'_1x'_2x'_3)\,(x'_1x'_2x'_4);\, x'_1\big) = \big(\alpha(abp);\, p\big).$$

Nach Axiom (III) müßte dann aber $\beta \in (abp)_p$ sein, was nicht der Fall ist. Da also $(\alpha\beta;\, q) \neq \big(\alpha(abp);\, a\big)$ ist und es nur zwei von 0 verschiedene freie Winkel gibt, ist $\big(\alpha(abp);\, a\big)$ durch den Winkel $(\alpha\beta;\, q)$ eindeutig bestimmt. Auf Grund dieser Bemerkung ist Hilfssatz 2. 4 vollends bewiesen.

Hilfssatz 2. 5. *Sind α, β Kreise durch die verschiedenen Punkte p, q und sind α', β' Kreise durch die verschiedenen Punkte p, q', dann sind die folgenden Aussagen äquivalent:*

(a) $\qquad (\alpha\beta;\, q) = (\alpha'\beta';\, q')$,

(b) $\qquad (\alpha\beta;\, p) = (\alpha'\beta';\, p)$.

Beweis. Im Falle $\alpha = \beta$ ist beidesmal $\alpha' = \beta'$, was die Behauptung für diesen Fall ergibt. Sei $\alpha \neq \beta$ und also $\alpha' \neq \beta'$. Aus (a) folgt (b): Seien $a \in \alpha - \beta$ und $a' \in \alpha' - \beta'$ feste Punkte. Dann gibt es nach Hilfssatz 2.4 Punkte $b \in \beta - \alpha$, $b' \in \beta' - \alpha'$ mit $\big(\alpha(abp);\, a\big) = \big(\alpha'(a'b'p);\, a'\big)$. Axiom (IV) angewandt mit den Bezeichnungen $(p, q, r) = (p, q, a)$, $(p', q', r') = (p, q', a')$ und $x_1 = p = x'_1$, $x_2 = q$, $x'_2 = q'$, $x_3 = a$, $x'_3 = a'$, $x_4 = b$, $x'_4 = b'$ führt auf (b).

Aus (b) folgt (a): Sei ξ der Kreis durch q', p mit $(\alpha\beta;\, q) = (\alpha'\xi;\, q')$. Mit der vorhin benutzten Schlußweise (aus (a) folgt (b)) ergibt sich hieraus $(\alpha\beta;\, p) = (\alpha'\xi;\, p)$. Wegen (b) ist also weiter $(\alpha'\beta';\, p) = (\alpha\beta;\, p) = (\alpha'\xi;\, p)$, d. h. $\xi = \beta'$ wegen $p, q' \in \xi \cap \beta'$ und $\xi \in \beta'_p$.

Hilfssatz 2. 6. *Sind $\alpha, \beta, \alpha', \beta'$ Kreise durch den Punkt p und gilt $(\alpha\beta; p) = (\alpha'\beta'; p)$, so gilt auch $(\beta\alpha; p) = (\beta'\alpha'; p)$.*

Beweis. Im Falle $\beta \in \alpha_p$ ist auch $\beta' \in \alpha'_p$ und also nichts mehr zu beweisen. Sei $\beta \notin \alpha_p$, $\beta' \notin \alpha'_p$. Sei $\alpha \cap \beta = \{p, q\}$, $q \neq p$, und $\alpha' \cap \beta' = \{p, q'\}$, $q' \neq p$. Wegen Hilfssatz 2. 5 ist also $(\alpha\beta; q) = (\alpha'\beta'; q')$. Wegen Hilfssatz 2. 4 gibt es zu vorgegebenen Punkten $a \in \alpha - \beta$, $a' \in \alpha' - \beta'$ weitere Punkte $b \in \beta - \alpha$, $b' \in \beta' - \alpha'$ mit $(\alpha(abp); a) = (\alpha'(a'b'p); a')$. Wir wenden jetzt Axiom (IV) an mit den Bezeichnungen $(p, q, r) = (p, q, a)$, $(p', q', r') = (p, q', a')$ und $x_1 = p = x'_1$, $x_2 = q$, $x'_2 = q'$, $x_3 = b$, $x'_3 = b'$, $x_4 = a$, $x'_4 = a'$. Dies ergibt die Behauptung.

Hilfssatz 2. 7 (*Korollar zu den Hilfssätzen* 2. 1 *und* 2. 6). *Sind α, β, γ Kreise durch einen Punkt p, so bilden die Lösungen λ von $(\alpha\beta; p) = (\lambda\gamma; p)$ genau ein Kontaktelement durch p. Ist q ein von p verschiedener Punkt, dann gibt es genau einen Kreis $\bar{\lambda} \ni p, q$ mit $(\alpha\beta; p) = (\bar{\lambda}\gamma; p)$.*

Hilfssatz 2. 8. *Sind $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ Kreise durch den Punkt t und gilt $(\alpha\beta; t) = (\alpha'\beta'; t)$, $(\beta\gamma; t) = (\beta'\gamma'; t)$, so gilt auch $(\gamma\alpha; t) = (\gamma'\alpha'; t)$.*

Beweis. Im Falle $\beta \in \alpha_t$ ist auch $\beta' \in \alpha'_t$, Dann ist

$$(\gamma\alpha; t) = (\gamma\beta; t) = (\gamma'\beta'; t) = (\gamma'\alpha'; t)$$

nach Hilfssatz 2. 6. Genau so erledigt sich der Fall $\gamma \in \beta_t$. Sei also $\beta \notin \alpha_t$, $\beta' \notin \alpha'_t$, $\gamma \notin \beta_t$, $\gamma' \notin \beta'_t$. Wir können auch $\gamma \notin \alpha_t (\gamma' \notin \alpha'_t)$ annehmen, da sich in diesem Falle die Behauptung einfach ergibt. Sei $\alpha \cap \beta = \{t, p\}$, $p \neq t$, und seien $\bar{\gamma}, \bar{\alpha}', \bar{\beta}', \bar{\gamma}'$ die durch $p \in \bar{\gamma} \in \gamma_t$, $p \in \bar{\alpha}' \in \alpha'_t$, $p \in \bar{\beta}' \in \beta'_t$, $p \in \bar{\gamma}' \in \gamma'_t$ eindeutig bestimmten Kreise. Mit Hilfssatz 2. 1 und Hilfssatz 2. 7 ist dann also $(\alpha\beta; t) = (\alpha'\beta'; t) = (\bar{\alpha}'\beta'; t) = (\bar{\alpha}'\bar{\beta}'; t)$, d. h. $(\beta\alpha; t) = (\bar{\beta}'\bar{\alpha}'; t)$ und $(\beta\bar{\gamma}; t) = (\beta'\gamma'; t) = (\bar{\beta}'\gamma'; t) = (\bar{\beta}'\bar{\gamma}'; t)$; weiterhin gilt $\alpha \neq \beta$, $\bar{\gamma} \neq \beta$, $\bar{\gamma} \neq \alpha$. Sind dann $b, \bar{b}'$ feste Punkte mit $b \in \beta - \alpha$, $\bar{b}' \in \bar{\beta}' - \bar{\alpha}'$, so gibt es nach Hilfssatz 2. 4 (es sei dort $q = t = q'$ gesetzt) Punkte $a \in \alpha - \beta$, $\bar{a}' \in \bar{\alpha}' - \bar{\beta}'$ mit $(\beta(bap); b) = (\bar{\beta}'(\bar{b}'\bar{a}'p); \bar{b}')$. Sicherlich gilt auch $b \in \beta - \bar{\gamma}$, $\bar{b}' \in \bar{\beta}' - \bar{\gamma}'$, da — etwa im Falle $b \in \bar{\gamma}$ — sich $\bar{\gamma} = (ptb) = \beta$ ergäbe. Dann existieren nach Hilfssatz 2. 4 Punkte $\bar{c} \in \bar{\gamma} - \beta$, $\bar{c}' \in \bar{\gamma}' - \bar{\beta}'$ mit $(\beta(b\bar{c}p); b) = (\bar{\beta}'(\bar{b}'\bar{c}'p); \bar{b}')$. Jetzt werde Axiom (IV) mit den Bezeichnungen $x_1 = t = x'_1$, $x_2 = p = x'_2$, $x_3 = \bar{c}$, $x_4 = a$, $x'_3 = \bar{c}'$, $x'_4 = \bar{a}'$ angewandt, wobei (vgl. die Bezeichnungen von Axiom (IV)) $(p, q, r) = (p, t, b)$, $(p', q', r') = (p, t, \bar{b}')$ gesetzt ist. Tatsächlich sind x_1, x_2, x_3, x_4 wegen $\bar{\gamma} \neq \alpha$ verschiedene Punkte; entsprechend sind x'_i wegen $\bar{\gamma}' \neq \bar{\alpha}'$ verschiedene Punkte. Da also weiter für x_3, x_4 die Bedingungen (c) von Axiom (IV) erfüllt sind, gilt $(\bar{\gamma}\alpha; t) = (\bar{\gamma}'\bar{\alpha}'; t)$. Mit den Hilfssätzen 2.1, 2.7 gilt weiter $(\gamma\alpha; t) = (\bar{\gamma}\alpha; t) = (\bar{\gamma}'\bar{\alpha}'; t) = (\gamma'\bar{\alpha}'; t) = (\gamma'\alpha'; t)$.

Hilfssatz 2. 9. *Es seien a, b, c, c' nicht gemeinsam auf einem Kreise gelegene Punkte. Ist dann z ein Punkt $\notin (abc)$, so gibt es genau einen Punkt $z' \in \xi \cap \eta - \{a\}$ mit*

$$((abc)\,(abz); a) = ((abc')\,\xi; a), \quad \xi \ni a, b,$$

$$((acb)\,(acz); a) = ((ac'b)\,\eta; a), \quad \eta \ni a, c'\ ^{10}).$$

Der Punkt z' liegt nicht auf (abc').

[10]) Zur besseren Veranschaulichung der angeschriebenen Gleichungen ersetze man sie durch die auf Grund von Hilfssatz 2. 5 äquivalenten Gleichungen $((abc)\,(abz); b) = ((abc')\,\xi; b)$, $((acb)\,(acz); c) = ((ac'b)\,\eta; c')$.

Beweis. Nach Hilfssatz 2. 1 sind die Kreise ξ, η eindeutig bestimmt. Es kann nicht $\eta \in \xi_a$ sein; man hätte sonst mit Axiom (III)

$$((abc)\,(abz);\,a) = ((abc')\,\xi;\,a) = ((ac'b)\,\eta;\,a) = ((acb)\,(acz);\,a),$$

d. h. $(abz) = (acz)$ nach Hilfssatz 2. 1, obwohl aber doch $z \notin (abc)$ ist. Wegen $\eta \notin \xi_a$ ist also $\xi \cap \eta = \{a, g\}$ für einen gewissen Punkt $g \neq a$. Es ist $g \neq b$, da sonst $(abc') = (agc') = \eta$ wäre und hiermit $0 = ((ac'b)\,\eta;\,a)) = ((acb)\,(acz);\,a)$, was wegen $(acb) \neq (acz)$ nicht der Fall ist. Weiter gilt $g \notin (abc')$. Man hätte sonst $\xi = (abg) = (abc')$, was $0 = ((abc')\,\xi;\,a) = ((abc)\,(abz);\,a)$ ergäbe. Man setze $g = z'$.

Satz 2. 4. *Es seien k, l, m, m' nicht gemeinsam auf einem Kreise gelegene Punkte und es sei für $x \notin (klm)$ eine Punktabbildung $x \to x' = f(x \mid k, l, m, m')$ definiert durch die Gleichungen*

$$((klm)\,(klx);\,k) = ((klm')\,(klx');\,k),$$
$$((kml)\,(kmx);\,k) = ((km'l)\,(km'x');\,k),\quad x' \notin \{k, l, m'\}.$$

Dann ist $x' = f(x \mid k, l, m, m')$ eine eineindeutige Abbildung von $\mathfrak{P} - (klm)$ auf $\mathfrak{P} - (klm')$.

Beweis. Läßt man in Hilfssatz 2. 9 die Punkte a, b, c, c', z nacheinander die Punkte k, l, m, m', x sein, so erkennt man, daß zu jedem Punkt $x \notin (klm)$ genau ein Bildpunkt $x' \notin (klm')$ existiert. $x \to x'$ ist eine eineindeutige Abbildung von $\mathfrak{P} - (klm)$ *in* $\mathfrak{P} - (klm')$: Angenommen, es gäbe verschiedene Punkte $x_1, x_2 \in \mathfrak{P} - (klm)$ mit $x_1' \equiv x' \equiv x_2'$. Dann ist also

$$((klm)\,(klx_1);\,k) = ((klm')\,(klx');\,k) = ((klm)\,(klx_2);\,k)$$

und

$$((kml)\,(kmx_1);\,k) = ((km'l)\,(km'x');\,k) = ((kml)\,(kmx_2);\,k),$$

was nach Hilfssatz 2. 1 aber $(klx_1) = (klx_2)$ und $(kmx_1) = (kmx_2)$ ergibt. Nun ist gewiß $(klx_i) \neq (kmx_i)$ für $i = 1, 2$, da sonst $x_i \in (klm)$ wäre. Damit ist

$$\{k, x_1\} = (klx_1) \cap (kmx_1) = (klx_2) \cap (kmx_2) = \{k, x_2\},$$

was entgegen der Voraussetzung $x_1 = x_2$ ergibt. — Jeder Punkt x' von $\mathfrak{P} - (klm')$ kommt als Bildpunkt eines Punktes $x \in \mathfrak{P} - (klm)$ vor: Läßt man zum Beweise in Hilfssatz 2. 9 die Punkte a, b, c, c', z nacheinander die Punkte k, l, m', m, x' sein, so gibt es also einen Punkt $x \in \mathfrak{P} - (klm)$ mit

$$((klm')\,(klx');\,k) = ((klm)\,(klx);\,k),$$
$$((km'l)\,(km'x');\,k) = ((kml)\,(kmx);\,k),$$

Diese Gleichungen zeigen aber unmittelbar, daß $x' = f(x \mid k, l, m, m')$ ist.

Hilfssatz 2. 10. *Es seien p, q, r, r' nicht gemeinsam auf einem Kreise gelegene Punkte. Dann gibt es genau einen Punkt r^0 mit*

(a) $$((pqr^0)\,(pqr);\,p) = ((pqr)\,(pqr');\,p),$$

(b) $$((pr^0q)\,(pr^0r);\,p) = ((prq)\,(prr');\,p),\quad r^0 \notin \{p, q, r\}.$$

Für r^0 gilt $r^0 \notin (pqr)$.

Beweis. Nach Hilfssatz 2. 7 gibt es genau einen Kreis $\mu \ni p, q$ mit

$$(\mu(pqr);\,p) = ((pqr)\,(pqr');\,p).$$

Nach Hilfssatz 2. 1 gibt es genau einen Kreis $\eta \ni p, r$ mit $(\mu\eta;\,p) = ((prq)\,(prr');\,p)$. Es kann nicht $\eta \in \mu_p$ sein, da nach Hilfssatz 2. 2 sonst $(prr') \in (prq)_p$, d. h. $(prr') = (prq)$ wäre. Es ist also $\eta \cap \mu = \{p, s\}$, $s \neq p$. Wir setzen $s = r^0$. Man hat $r^0 \neq q$, da sonst $\eta = (pqr)$ wäre wegen $q = r^0 \in \eta$ und damit

$$((prq)\,(prr');\,p) = (\mu\eta;\,p) = (\mu(pqr);\,p) = ((pqr)\,(pqr');\,p),$$

was $(prr') = (pqr')$ ergäbe. Weiter ist $r^0 \notin (pqr)$. Es wäre sonst $\mu = (pqr^0) = (pqr)$ und hiermit

$$0 = (\mu(pqr);\, p) = ((pqr)\,(pqr');\, p), \text{ d. h. } (pqr) = (pqr').$$

Verschiedene Punkte r_1^0, r_2^0 mit den gewünschten Eigenschaften kann es nicht geben, da $r_1^0, r_2^0 \in \xi \cap \mu - \{p\}$ sein muß, was $r_1^0 = r_2^0$ ergibt.

Definition. *Es seien p, q, r, r' nicht gemeinsam auf einem Kreise gelegene Punkte und es sei r^0 der gemäß Hilfssatz 2. 10 den Punkten p, q, r, r' eindeutig zugeordnete Punkt. Dann wird mit*

$$x \to x' = F(x \mid p, q, r, r')$$

die folgende Punktabbildung bezeichnet:

$$x' = \begin{cases} f(x \mid p, q, r, r') & x \notin (pqr) \\ f(x \mid p, q, r^0, r) \quad \text{für} & x \in (pqr) - \{p, q\} \\ x & x \in \{p, q\}. \end{cases}$$

Es gilt

Satz 2. 5. 1. *Die Abbildung $x' = F(x \mid p, q, r, r')$ ist eine eineindeutige Abbildung von $\mathfrak{P}$ auf sich.*

Beweis. Läßt man in Satz 2. 4 die Punkte k, l, m, m' nacheinander die Punkte p, q, r, r' sein, so sieht man, daß $x' = f(x \mid p, q, r, r')$ eine eineindeutige Abbildung von $\mathfrak{P} - (pqr)$ auf $\mathfrak{P} - (pqr')$ ist. Wir haben also noch zu zeigen:

$$x' = \begin{cases} f(x \mid p, q, r^0, r) & \text{für} \quad x \in (pqr) - \{p, q\} \\ x & \phantom{\text{für}} \quad x \in \{p, q\} \end{cases}$$

ist eine eineindeutige Abbildung von (pqr) auf (pqr'). — Wegen Satz 2. 4 (man setze $k = p$, $l = q$, $m = r^0$, $m' = r$ und beachte $r^0 \notin (pqr)$) ist $x' = f(x \mid p, q, r^0, r)$ eine eineindeutige Abbildung von $\mathfrak{P} - (pqr^0)$ auf $\mathfrak{P} - (pqr)$. Es ist also lediglich zu zeigen, daß $(pqr) \cap (\mathfrak{P} - (pqr^0)) = (pqr) - \{p, q\}$ gilt — dies folgt sofort aus $r^0 \notin (pqr)$ — und daß $x' \in (pqr') - \{p, q\}$ für die Punkte $x \in (pqr) - \{p, q\}$ bzw. $x \in (pqr) - \{p, q\}$ für die Punkte $x' \in (pqr') - \{p, q\}$ gilt. Sei $x \in (pqr) - \{p, q\}$. Dann ist also $((pqr^0)\,(pqx);\, p) = ((pqr)\,(pqx');\, p)$. Beachtet man $(pqx) = (pqr)$ und (vgl. Hilfssatz 2. 10) $((pqr^0)\,(pqr);\, p) = ((pqr)\,(pqr');\, p)$, so ist also $((pqr)\,(pqr');\, p) = ((pqr)\,(pqx');\, p)$, d. h. $(pqr') = (pqx')$, d. h. $x' \in (pqr')$. Sei umgekehrt ein Punkt $x' \in (pqr') - \{p, q\}$ gegeben: Wegen $(pqr') = (pqx')$ ist dann $((pqr^0)\,(pqx);\, p) = ((pqr^0)\,(pqr);\, p)$, d. h. $(pqx) = (pqr)$, d. h. $x \in (pqr)$.

Anmerkung zu Satz 2. 5. 1. Die Abbildung $x' = F(x \mid p, q, r, r')$ überführt r nach r' und r^0 nach r.

Beweis. a) $r \to r'$: Wegen $r \in (pqr) - \{p, q\}$ ist das Bild $\bar{r}$ von r durch

$$\bar{r} = f(r \mid p, q, r^0, r)$$

gegeben, d. h. durch $((pqr^0)\,(pqr);\, p) = ((pqr)\,(pqr);\, p)$, $((pr^0q)\,(pr^0r);\, p) = ((prq)\,(prr);\, p)$.

Vergleicht man diese Beziehungen mit den Gleichungen von Hilfssatz 2. 10, so erkennt man unter Benutzung von Hilfssatz 2. 9 die Behauptung $\bar{r} = r'$.

b) $r^0 \to r$: Wegen $r^0 \notin (pqr)$ ist das Bild $\overline{r^0}$ von r^0 durch $\overline{r^0} = f(r^0 \mid p, q, r, r')$ gegeben, d. h. durch $((pqr)\,(pqr^0);\, p) = ((pqr')\,(pq\overline{r^0});\, p)$, $((prq)\,(prr^0);\, p) = ((pr'q)\,(pr'\overline{r^0});\, p)$. Schreibt man die r^0 definierenden Gleichungen von Hilfssatz 2. 10 vermöge der Hilfssätze 2.6, 2.8 um: $((pqr)\,(pqr^0);\, p) = ((pqr')\,(pqr);\, p)$, $((prq)\,(prr^0);\, p) = ((pr'q)\,(pr'r);\, p)$, so erkennt man $\overline{r^0} = r$ mit Hilfssatz 2. 9.

Satz 2. 5. 2. *Es seien p, q, r, r' nicht gemeinsam auf einem Kreise gelegene Punkte und es seien s, s' Punkte mit $s \notin (pqr)$ und $s' = F(s \mid p, q, r, r')$. Dann ist $F(x \mid p, q, r, r') = F(x \mid p, q, s, s')$ für alle $x \in \mathfrak{P}$.*

Zum Beweise zeigen wir zunächst

Hilfssatz 2. 11. 1. *Es seien p, q, u, u' nicht gemeinsam auf einem Kreise gelegene Punkte und es seien v, v' Punkte mit $v \notin (pqu)$ und $v' = f(v \mid p, q, u, u')$. Ist dann x ein Punkt mit $x \notin (pqu), (pqv)$, so ist $f(x \mid p, q, u, u') = f(x \mid p, q, v, v')$.*

Beweis. Setzen wir $x'_u = f(x \mid p, q, u, u')$, $x'_v = f(x \mid p, q, v, v')$, so gilt $((pqv)\,(pqx);\, p) = ((pqv')\,(pqx'_u);\, p)$ wegen $((pqu)\,(pqx);\, p) = ((pqu')\,pqx'_u);\, p)$ und $((pqu)\,(pqv);\, p) = ((pqu')\,(pqv');\, p)$ auf Grund der Hilfssätze 2. 6, 2. 8. Weiterhin wenden wir Axiom (IV) an, indem wir $(p, q, r) = (p, q, u)$, $(p, q', r') = (p, q, u')$ und $x_1 = p = x'_1$, $x_2 = v$, $x'_2 = v'$, $x_3 = q = x'_3$, $x_4 = x$, $x'_4 = x'_u$ setzen. Zunächst sind $x_1, \ldots, x_4$ und $x'_1, \ldots, x'_4$ je vier verschiedene Punkte: Es ist $x \notin (pqv)$. Da $y \to f(y \mid p, q, u, u')$ nach Satz 2. 4 eine eineindeutige Abbildung von $\mathfrak{P} - (pqu)$ auf $\mathfrak{P} - (pqu')$ ist, ist wegen $v \notin (pqu)$ und $x \notin (pqu)$ sicher $v' \notin (pqu')$ und $x'_u \notin (pqu')$; wegen $x \neq v$ ist $x'_u \neq v'$. Die Eigenschaft (c) ist wegen $v' = f(v \mid p, q, u, u')$, $x'_u = f(x \mid p, q, u, u'$ und Hilfssatz 2. 5 auch erfüllt. Axiom (IV) ergibt dann $((pvq)\,(pvx);\, p) = ((pv'q)\,(pv'x'_u);\, p)$. Vergleicht man die Gleichungen

$$((pqv)\,(pqx);\, p) = ((pqv')\,(pqx'_u);\, p),\quad ((pvq)\,(pvx);\, p) = ((pv'q)\,(pv'x'_u);\, p)$$

mit $x'_v = f(x \mid p, q, v, v')$, so erkennt man $x'_u = x'_v$ mit Hilfssatz 2. 9.

Hilfssatz 2. 11. 2. *Es seien p, q, g, g' nicht gemeinsam auf einem Kreise gelegene Punkte und es seien h, h' Punkte mit $h \notin (pqg)$, $h \in (pqg^0)$ und $h' = f(h \mid p, q, g, g')$. Ist dann x ein Punkt mit $x \in (pqg)$, $x \notin (pqh)$, so folgt $f(x \mid p, q, g^0, g) = f(x \mid p, q, h, h')$.*

Beweis. $h' = f(h \mid p, q, g, g')$, die Definitionsgleichungen von g^0, $x'_g = f(x \mid p, q, g^0, g)$, $x'_h = f(x \mid p, q, h, h')$ führen auf

2. 11. 2. 1.	$((pqg)\,(pqh);\, p)$	$= ((pqg')\,(pqh');\, p)$,
2. 11. 2. 2.	$((pgq)\,(pgh);\, p)$	$= ((pg'q)\,(pg'h');\, p)$,
2. 11. 2. 3.	$((pqg^0)\,(pqg);\, p)$	$= ((pqg)\,(pqg');\, p)$,
2. 11. 2. 4.	$((pg^0q)\,(pg^0g);\, p)$	$= ((pgq)\,(pgg');\, p)$,
2. 11. 2. 5.	$((pqg^0)\,(pqx);\, p)$	$= ((pqg)\,(pqx'_g);\, p)$,
2. 11. 2. 6.	$((pg^0q)\,(pg^0x);\, p)$	$= ((pgq)\,(pgx'_g);\, p)$,
2. 11. 2. 7.	$((pqh)\,(pqx);\, p)$	$= ((pqh')\,(pqx'_h);\, p)$,
2. 11. 2. 8.	$((phq)\,(phx);\, p)$	$= ((ph'q)\,(ph'x'_h);\, p)$.

Es ist $h' \in (pqg)$: Wegen $h \in (pqg^0)$, $h \notin (pqg)$ ist $(pqg^0) = (pqh)$. 2. 11. 2. 3 kann deshalb in der Form $((pqh)\,(pqg);\, p) = ((pqg)\,(pqg');\, p)$ geschrieben werden. Mit 2. 11. 2. 1 folgt hieraus $((pqg)\,(pqg');\, p) = ((pqh)\,(pqg);\, p) = ((pqh')\,(pqg');\, p)$, was $(pqg) = (pqh')$ ergibt.

Weiterhin gilt $x'_g \in (pqg') \ni x'_h$: Aus 2. 11. 2. 3 und 2. 11. 2. 5 folgt

$$((pqg)\,(pqx);\, p) = ((pqg')\,(pqx'_g);\, p)$$

vermittels der Hilfssätze 2. 6, 2. 8. Wegen $(pqg) = (pqx)$ ist also $(pqg') = (pqx'_g)$. Aus 2. 11. 2. 1 und 2. 11. 2. 7 folgt $((pqg)\,(pqx);\, p) = ((pqg')\,(pqx'_h);\, p)$. Auf Grund von $(pqg) = (pqx)$ ist $(pqg') = (pqx'_h)$.

Wegen $(pg^0q) = (phq)$ und $(pgq) = (ph'q)$ folgt aus 2. 11. 2. 6 und 2. 11. 2. 8

$$\big((pg^0x)\,(phx);\,p\big) = \big((pgx'_g)\,(ph'x'_h);\,p\big).$$

Ist $(ph'x'_h) \in (pgx'_g)_p$, so folgt $(pg^0x) = (phx)$, was $g^0 = h$ bedeutet, da sonst $x \in (pqh)$ sein müßte. Auf Grund der Anmerkung zu Satz 2. 5. 1 ist im Falle $g^0 = h$ aber $g = h'$, was $(ph'x'_h) = (pgx'_g)$ zur Folge hat. Nun ist

$$\{x'_g\} = (pqg') \cap (pgx'_g) - \{p\} \equiv (pqg') \cap (ph'x'_h) - \{p\} = \{x'_h\},$$

womit die Behauptung in diesem Sonderfall bewiesen ist. Auch der Sonderfall $x = g$ ist leicht erledigt. Dann ist nämlich $x'_g = g'$. 2. 11. 2. 8 gibt weiterhin $\big((phq)\,(phg);\,p\big) = \big((ph'q)\,(ph'x'_h);\,p\big)$, was (vgl. 2. 11. 2. 1 und 2, 11. 2. 2) mit

2. 11. 2. 9. $$\big((phq)\,(phg);\,p\big) = \big((pqh')\,(pg'h');\,p\big)$$

auf $(ph'x'_h) = (pg'h')$, d. h. auf $\{x'_h\} = (pqg') \cap (ph'x'_h) - \{p\} \equiv (pqg') \cap (pg'h') - \{p\} = \{g'\}$ führt.

Sei im folgenden $g^0 \neq h$ und $x \neq g$. Dann ist also $(ph'x'_h) \notin (pgx'_g)_p$. Es gibt also einen Punkt $j \neq p$ mit $(ph'x'_h) \cap (pgx'_g) = \{p, j\}$. Ist $j \in (pqg')$, so sind wir fertig, da — etwa im Fall $j \neq x'_g$ — sich $(pqg') = (px'_gj) = (pgx'_g)$, d. h. $g' \in (pqg)$ ergäbe. Wir zeigen nun $j \in (pqg')$: Dies geschieht mit Axiom (IV), wobei $(p, q, r) = (p, g^0, h)$ gesetzt ist (das hier angeschriebene q ist das in Axiom (IV) benutzte; es ist nicht mit dem im bisherigen Beweisgang auftretenden q zu verwechseln), ferner $(p', q', r') = (p, g, h')$ und weiter $x_1 = g$, $x'_1 = g'$, $x_2 = p = x'_2$, $x_3 = x$, $x'_3 = j$, $x_4 = h$, $x'_4 = h'$. Mit $g^0 \neq h$ und der hieraus folgenden Aussage $g \neq h'$ sind also p, g^0, h und p, g, h' je drei verschiedene Punkte. $x_1, \ldots, x_4$ sind wegen $x \neq g$ verschiedene Punkte. $x'_1, \ldots, x'_4$ können als verschieden angenommen werden, da im Falle $j = g'$ ja $j \in (pqg')$ ist. Für die Bedingung (a) von Axiom (IV) überlegen wir uns noch $j \notin (pgh')$: Angenommen, es wäre $j \in (pgh')$. Es ist $j \neq g$, da sonst $g \in (ph'x'_h)$, d. h. $x'_h \in (pgh') = (pqg)$ wäre. Dann müßte $x'_g \in (pgj) = (pgh')$ sein, was nicht der Fall ist. Die Gleichungen (c) entnimmt man (unter Berücksichtigung von Hilfssatz 2. 5) den Gleichungen

2. 11. 2. 6 (man beachte $(pg^0q) = (pg^0h)$, $(pgq) = (pgh')$ und $(pgx'_g) = (pgj)$), also

$$\big((pg^0h)\,(pg^0x);\,p\big) = \big((pgq)\,(pgx'_g);\,p\big) = \big((pgh')\,(pgj);\,p\big),$$

2. 11. 2. 8 (man beachte $(phq) = (pg^0h)$, $(pgh') = (ph'q)$ und $(ph'x'_h) = (ph'j)$), also

$$\big((pg^0h)\,(phx);\,p\big) = \big((pgh')\,(ph'j);\,p\big),$$

2. 11. 2. 4, also

$$\big((pg^0h)\,(pg^0g);\,p\big) = \big((pgh')\,(pgg');\,p\big),$$

2. 11. 2. 9, also

$$\big((phg^0)\,(phg);\,p\big) = \big((pgh')\,(pg'h');\,p\big).$$

Axiom (IV) ergibt daher

$$\big((pgx)\,(pgh);\,g\big) = \big((pg'j)\,(pg'h');\,g'\big) \text{ bzw. } \big((pqg)\,(pgh);\,g\big) = \big((pg'j)\,(pg'h');\,g'\big),$$

was mit 2. 11. 2. 2 auf $(pg'q) = (pg'j)$, d. h. auf $j \in (pqg')$ führt.

Nun zum *Beweise von Satz* 2. 5. 2.

Die Bedingung $F(x \mid p, q, r, r') = F(x \mid p, q, s, s')$ ist gewiß erfüllt für $x = p$ und $x = q$. Wir unterscheiden die folgenden weiteren Fälle:

1) $x \notin (pqr)$, $x \notin (pqs)$.

Setzen wir $u = r$, $u' = r'$, $v = s$, $v' = s'$ in Hilfssatz 2. 11. 1, so haben wir

$$F(x \mid p, q, r, r') \equiv f(x \mid p, q, r, r') = f(x \mid p, q, s, s') \equiv F(x \mid p, q, s, s').$$

2) $x \in (pqr)$, $x \notin (pqs)$.

2_1. $s \in (pqr^0)$. Setzen wir $g = r$, $g' = r'$, $h = s$, $h' = s'$ in Hilfssatz 2. 11. 2, so folgt

$$F(x \mid p, q, r, r') \equiv f(x \mid p, q, r^0, r) = f(x \mid p, q, s, s') \equiv F(x \mid p, q, s, s').$$

2_2. $s \notin (pqr^0)$. Wir setzen $u = r^0$, $u' = r$, $v = s$, $v' = s'$ in Hilfssatz 2. 11. 1. Wegen Hilfssatz 2. 10 liegen die Punkte p, q, r^0, r nicht gemeinsam auf einem Kreise. Es ist weiter $s' = f(s \mid p, q, r^0, r)$: Zum Beweise wenden wir Axiom (IV) an, wobei die dort benutzten Punkte p, q, r, r' mit den hier benutzten p, q, r, r' übereinstimmen sollen. Weiter sei gesetzt $x_1 = p = x_1'$, $x_2 = r^0$, $x_2' = r$, $x_3 = q = q' = x_3'$, $x_4 = s$, $x_4' = s'$. Wegen $s \notin (pqr^0)$ sind $x_1, \ldots, x_4$ verschiedene Punkte; wegen $s \neq r^0$ gilt $s' \equiv f(s \mid p, q, r, r') \neq r$ und also $|\{x_1', \ldots, x_4'\}| = 4$. Die Bedingungen (a), (b) von Axiom (IV) gelten offensichtlich. Zu (c): Auf Grund von $s' = f(s \mid p, q, r, r')$ ist mit Hilfssatz 2. 5

$$((pqr)\,(pqs);\, q) = ((pqr')\,(pqs');\, q),\quad ((prq)\,(prs);\, r) = ((pr'q)\,(pr's');\, r').$$

Auf Grund von $r = f(r^0 \mid p, q, r, r')$ ist ebenfalls mit Hilfssatz 2. 5

$$((pqr)\,(pqr^0);\, q) = ((pqr')\,(pqr);\, q),\quad ((prq)\,(prr^0);\, r) = ((pr'q)\,(pr'r);\, r').$$

Axiom (IV) ergibt also

$$(*)\qquad ((pr^0q)\,(pr^0s);\, p) = ((prq)\,(prs');\, p).$$

Aus den jeweils ersten Gleichungen der beiden zuletzt angeschriebenen Gleichungspaare ergibt sich noch

$$(**)\qquad ((pqr^0)\,(pqs);\, p) = ((pqr)\,(pqs');\, p)$$

unter Berücksichtigung der Hilfssätze 2. 5, 2. 6, 2. 8. Setzen wir nun $s_1' \equiv f(s \mid p, q, r^0, r)$, so erkennt man $s' = s_1'$ mit Hilfssatz 2. 9 und den Gleichungen (*), (**). Wegen $s' = f(s \mid p, q, r^0, r)$ folgt nun aus Hilfssatz 2. 11. 1 — wenn man noch $x \notin (pqr^0)$ wegen $x \in (pqr) - \{p, q\}$ beachtet —

$$F(x \mid p, q, r, r') \equiv f(x \mid p, q, r^0, r) = f(x \mid p, q, s, s') \equiv F(x \mid p, q, s, s').$$

3) $x \notin (pqr)$, $x \in (pqs)$.

Dies ist bis auf die Bezeichnung der Fall 2), wenn man voranschickt, daß p, q, s, s' nicht gemeinsam auf einem Kreise gelegene Punkte sind und weiterhin, daß $r \notin (pqs)$ und $r' = F(r \mid p, q, s, s')$ ist.

4) $x \in (pqr)$, $x \in (pqs)$.

Es ist dann $x \in \{p, q\}$.

Damit ist Satz 2. 5. 2 vollends bewiesen.

In Ergänzung von Satz 2. 3 können wir jetzt beweisen:

Satz 2. 6. *Sind a, b, c verschiedene Punkte, ebenso a', b', c', dann gibt es mindestens (mit Satz 2. 3 also genau) eine Abbildung $\tau \in T(\Sigma)$, für die $(a, b, c)^\tau = (a', b', c')$ ist.*

Der Beweis wird in mehreren Schritten erbracht.

2. 6. 1. *Sind p, q, r, r' nicht gemeinsam auf einem Kreise gelegene Punkte, so gibt es ein $\tau \in T(\Sigma)$ mit $(p, q, r)^\tau = (p, q, r')$.*

Beweis. Die Abbildung σ: $x \to F(x \mid p, q, r, r')$ überführt p in p, q in q und r in r'. Nach Satz 2. 5. 1 ist sie eine umkehrbar eindeutige Abbildung der Menge der Punkte von Σ auf sich. Sie ist aber auch kreisverwandt und winkeltreu, also Element von $T(\Sigma)$: Sei zum Beweise $\mathfrak{x} = \{x_1, x_2, x_3, x_4\}$ eine Menge von irgend vier verschiedenen Punkten. Es gibt dann einen Punkt $s \neq p, q$ mit

(a) $(pqs) - \{p, q\}$ enthält höchstens einen Punkt von $\mathfrak{x}$.

(b) $s \in \mathfrak{x}$ für $|[(pqs) - \{p, q\}] \cap \mathfrak{x}| = 1$.

(c) $s = r$ für $s \in (pqr)$.

Liegt nicht die Minimalebene — bestehend aus fünf verschiedenen Punkten und zehn verschiedenen Kreisen — vor, so gibt es durch zwei verschiedene Punkte wenigstens vier verschiedene Kreise. Es gibt also durch p, q wenigstens drei verschiedene Kreise $\alpha, \beta, \gamma \neq (pqr)$. Würde nun jeder dieser Kreise α, β, γ mindestens zwei verschiedene Punkte von $\mathfrak{x} - \{p, q\}$ enthalten, so müßte $|\mathfrak{x} - \{p, q\}| \geqq 6$ sein. Es gibt also wenigstens einen Kreis — er sei etwa α — mit $|(\alpha - \{p, q\}) \cap \mathfrak{x}| \leqq 1$. Enthält er einen Punkt aus $\mathfrak{x} - \{p, q\}$, so sei dieser gleich s gesetzt. Im anderen Falle sei s irgendein Punkt von $\alpha - \{p, q\}$. Liegt die Minimalebene vor, so besitzt jeder Kreis genau drei verschiedene Punkte. Wir können dann immer $s = r$ setzen. Unter s' verstehen wir nun den Punkt $F(s \mid p, q, r, r')$. Dann kann die Abbildung σ: $x \to F(x \mid p, q, r, r')$ nach Satz 2. 5. 2 auch als σ: $x \to F(x \mid p, q, s, s')$ geschrieben werden, wobei also

$$|(\mathfrak{x} - \{p, q\}) \cap (pqs)| = \begin{cases} 0 \\ 1 \end{cases} \text{ist für } \begin{matrix} s \notin \mathfrak{x} \\ s \in \mathfrak{x} \end{matrix}.$$

Ist $\mathfrak{x}$ konzyklisch, so wenden wir Axiom (IV) an: Es seien die dortigen Bezeichnungen in folgender Weise verwendet: $(p, q, r) = (p, q, s)$, $(p, q, r') = (p, q, s')$. Die x_i seien die hier benutzten. x_i' sei gleich $F(x_i \mid p, q, s, s')$. Dann ist also

$$0 = ((x_1 x_2 x_3)(x_1 x_2 x_4); x_1) = ((x_1^\sigma x_2^\sigma x_3^\sigma)(x_1^\sigma x_2^\sigma x_4^\sigma); x_1^\sigma).$$

Damit ist $\mathfrak{x}^\sigma = \{x_1^\sigma, \ldots, x_4^\sigma\}$ auch konzyklisch. Die gleiche Schlußweise überträgt sich auf den Fall, daß $\mathfrak{x}$ nicht konzyklisch ist. σ ist also eine Kreisverwandtschaft.

Wir zeigen, daß σ auch kreiswinkeltreu ist, d. h., daß $\sigma \in T(\Sigma)$ gilt. Ist $(\xi\eta; x_1)$ ein beliebiger Winkel, so haben wir $(\xi\eta; x_1) = (\xi^\sigma \eta^\sigma; x_1^\sigma)$ zu zeigen. Für $\eta \in \xi_{x_1}$ ist dies klar, da für eine Kreisverwandtschaft σ stets $\eta^\sigma \in \xi^\sigma_{x_1^\sigma}$ folgt. Ebenfalls ist dies klar für $\eta^\sigma \in \xi^\sigma_{x_1^\sigma}$, da σ^{-1} Kreisverwandtschaft ist. Sei $\eta \notin \xi_{x_1}$ und $\eta^\sigma \notin \xi^\sigma_{x_1^\sigma}$. Sei also $\xi \cap \eta = \{x_1, x_2\}$, $x_2 \neq x_1$, und $\xi^\sigma \cap \eta^\sigma = \{x_1^\sigma, z\}$. Da die Beziehung $x_2 \in \xi \cap \eta - \{x_1\}$ in $x_2^\sigma \in \xi^\sigma \cap \eta^\sigma - \{x_1^\sigma\}$ übergehen muß, ist $z = x_2^\sigma$. Seien jetzt x_3, x_4 Punkte mit $x_3 \in \xi - \eta$, $x_4 \in \eta - \xi$. Dann ist $x_3^\sigma \in \xi^\sigma - \eta^\sigma$ und $x_4^\sigma \in \eta^\sigma - \xi^\sigma$.

Bestimmen wir zu den Punkten $x_1, \ldots, x_4$ jetzt wieder einen Punkt s mit $|(\mathfrak{x} - \{p, q\}) \cap (pqs)| = \begin{cases} 0 \\ 1 \end{cases}$ für $\begin{matrix} s \notin \mathfrak{x} \\ s \in \mathfrak{x} \end{matrix}$, und ersetzen wir wieder $F(x \mid p, q, r, r')$ durch $F(x \mid p, q, s, s')$, so ergibt Axiom (IV) mit (p, q, s), (p, q, s') als Grundtripel

$$(\xi\eta; x_1) = ((x_1 x_2 x_3)(x_1 x_2 x_4); x_1) = ((x_1^\sigma x_2^\sigma x_3^\sigma)(x_1^\sigma x_2^\sigma x_4^\sigma); x_1^\sigma) = (\xi^\sigma \eta^\sigma; x_1^\sigma).$$

2. 6. 2. *Sind p, q, r, r' gemeinsam auf einem Kreise gelegene, verschiedene Punkte, so gibt es eine Abbildung $\tau \in T(\Sigma)$, die p und q festläßt und die r in r' überführt.*

Beweis. Gemäß dem Reichhaltigkeitsaxiom einer $[M]$-Ebene gibt es einen Punkt $s \notin (pqr)$. Nach 2. 6. 1 gibt es dann eine Abbildung $\tau_1 \in T(\Sigma)$, die p und q festläßt und die r in s überführt. Da die Punkte p, q, s, r' nicht konzyklisch sind, gibt es eine Abbildung $\tau_2 \in T(\Sigma)$, die p und q festläßt und die s in r' überführt. Da $T(\Sigma)$ Gruppe ist, gilt $\tau_1\tau_2 \in T(\Sigma)$. Es ist aber $p^{\tau_1\tau_2} = p$, $q^{\tau_1\tau_2} = q$, $r^{\tau_1\tau_2} = (r^{\tau_1})^{\tau_2} = s^{\tau_2} = r'$.

Auf Grund von Satz 2. 3 und 2. 6. 1 und 2. 6. 2 haben wir:

2. 6. 3. *Sind p, q, r, r' verschiedene Punkte, so gibt es genau eine kreiswinkeltreue Kreisverwandtschaft τ mit $(p, q, r)^\tau = (p, q, r')$.*

Wir zeigen weiter

2. 6. 4. *Sind a, b, c verschiedene Punkte und ebenso a, b', c', dann gibt es eine Abbildung $\tau \in T(\Sigma)$ mit $(a, b, c)^\tau = (a, b', c')$.*

Beweis. 1. *Fall*: $c' = b$. Da eine $[M]$-Ebene wenigstens fünf verschiedene Punkte besitzt, gibt es einen Punkt $s \neq a, b, c, b'$. Wegen 2. 6. 3 gibt es eine Abbildung $\tau_1 \in T(\Sigma)$ mit $(a, b, c)^{\tau_1} = (a, s, c)$. Ebenfalls nach 2. 6. 3 gibt es Abbildungen $\tau_2, \tau_3 \in T(\Sigma)$ mit $(a, s, c)^{\tau_2} = (a, s, b)$ und $(a, s, b)^{\tau_3} = (a, b', b)$, wenn man beachtet, daß $a, b', c' = b$, d. h. daß s, a, b', b verschiedene Punkte sind. Damit ist $\tau_1\tau_2\tau_3 \in T(\Sigma)$ und

$$(a, b, c)^{\tau_1\tau_2\tau_3} = (a, b', b = c').$$

2 *Fall*: $c' \neq b$. Wir können auch $b' \neq c$ annehmen, da sonst bis auf die Bezeichnung Fall 1 vorläge. Ebenfalls setzen wir $b' \neq b$ und $c' \neq c$ voraus. Damit sind die Punkte a, b, c, b', c' paarweise verschieden. Es seien dann τ_1, τ_2 nach 2. 6. 3 existierende Abbildungen aus $T(\Sigma)$ mit $(a, b, c)^{\tau_1} = (a, b, c')$, $(a, b, c')^{\tau_2} = (a, b', c')$. Damit ist $\tau_1\tau_2 \in T(\Sigma)$ und $(a, b, c)^{\tau_1\tau_2} = (a, b', c')$.

Damit kommen wir zum Abschluß des Beweises von Satz 2. 6:

2. 6. 5. *Sind a, b, c verschiedene Punkte und ebenso a', b', c', dann gibt es ein $\tau \in T(\Sigma)$ mit $(a, b, c)^\tau = (a', b', c')$.*

Beweis. Sind a, b', c' verschiedene Punkte, so gibt es nach 2.6.4 eine Abbildung $\tau_1 \in T(\Sigma)$ mit $(a,b,c)^{\tau_1} = (a,b',c')$. Ebenfalls nach 2. 6. 4 gibt es eine Abbildung $\tau_2 \in T(\Sigma)$ mit $(b',a,c')^{\tau_2} = (b',a',c')$. Dann ist weiter $\tau_1\tau_2 \in T(\Sigma)$ und $(a,b,c)^{\tau_1\tau_2} = (a', b', c')$; dies ist die Behauptung für den genannten Spezialfall. — Die gleiche Schlußweise kann man anwenden, wenn a', b, c' oder a', b', c verschiedene Punkte sind. Wir können also $a \in \{b', c'\}$ $b \in \{a', c'\}$, $c \in \{a', b'\}$ annehmen. Ist $a = c'$, so muß — da a, b, c verschiedene Punkte sind — $b = a'$ und $c = b'$ sein. In diesem Falle seien $\tau_1, \tau_2 \in T(\Sigma)$ nach 2. 6. 4 existierende Abbildungen mit $(a, b, c)^{\tau_1} = (a, c, b)$ und $(a, c, b)^{\tau_2} = (b, c, a)$; es folgt $\tau_1\tau_2 \in T(\Sigma)$ und $(a, b, c)^{\tau_1\tau_2} = (b, c, a)$. Der noch verbleibende Fall $a = b'$, $b = c'$, $c = a'$ ist bis auf die Bezeichnung der gerade abgehandelte.

Der folgende Satz stellt eine weitere Brücke zwischen $T(\Sigma)$ und der betrachteten Winkelvergleichung dar.

Satz 2. 7. *Sind α, β Kreise durch den Punkt p mit $\beta \notin \alpha_p$ und sind γ, δ Kreise durch den Punkt q, so ist $(\alpha\beta; p) = (\gamma\delta; q)$ genau dann erfüllt, wenn es eine Abbildung $\tau \in T(\Sigma)$ mit $(\alpha, \beta, p)^\tau = (\gamma, \delta, q)$ gibt.*

Beweis. Auf Grund der Definition von $T(\Sigma)$ ist nur zu beweisen, daß aus $(\alpha\beta; p) = (\gamma\delta; q)$ die Existenz einer Abbildung $\tau \in T(\Sigma)$ mit $(\alpha, \beta, p)^\tau = (\gamma, \delta, q)$ folgt. Wegen $\beta \notin \alpha_p$ gibt es einen Punkt $\overline{p} \neq p$ mit $\alpha \cap \beta = \{p, \overline{p}\}$. Gewiß ist $\delta \notin \gamma_q$. Sei also $\gamma \cap \delta = \{q, \overline{q}\}$, $\overline{q} \neq q$. Es bezeichne a einen Punkt auf α, der nicht auf β liegt; ebenso sei c ein Punkt mit $c \in \gamma - \delta$. Dann sei τ die Abbildung aus $T(\Sigma)$ mit $(p, \overline{p}, a)^\tau = (q, \overline{q}, c)$. Offenbar ist dann $(\alpha\beta; p) = (\gamma\beta^\tau; q)$, was zusammen mit $(\alpha\beta; p) = (\gamma\delta; q)$ auf $(\gamma\delta; q) = (\gamma\beta^\tau; q)$ führt. Aus Axiom (III) folgt $\beta^\tau \in \delta_q$; beachtet man noch $\beta^\tau \cap \delta > \{q, \overline{q}\}$, so hat man insgesamt $\beta^\tau = \delta$. Damit gibt es tatsächlich eine Abbildung $\tau \in T(\Sigma)$ mit $(\alpha, \beta, p)^\tau = (\gamma, \delta, q)$.

Im folgenden Satz kennzeichnen wir die $[M]$-Ebenen, in denen eine Winkelvergleichung in der Stärke (I) bis (IV) gegeben ist, durch gruppentheoretisch-geometrische Eigenschaften. Wir gehen aus von einer $[M]$-Ebene Σ, die eine Gruppe T von Kreisverwandtschaften besitzt mit:

(T 1) *Sind a, b, c drei verschiedene Punkte und ebenso a', b', c', dann gibt es genau eine Abbildung $\tau \in T$ mit $(a, b, c)^\tau = (a', b', c')$.*

(T 2) *Sind α, β Kreise durch den Punkt p und ist τ eine Abbildung aus T mit $(\alpha, p)^\tau = (\alpha, p)$, so gilt $\beta^\tau \in \beta_p$*[11]).

Dann beweisen wir den

Satz 2. 8. *In Σ gibt es eine Winkelvergleichung „=" in der Stärke* (I) *bis* (IV). *Die durch diese Winkelvergleichung induzierte Gruppe $T(\Sigma)$ der kreiswinkeltreuen Kreisverwandtschaften ist isomorph zu unserer Ausgangsgruppe T.*

Der Beweis von Satz 2. 8 wird in mehreren Schritten erbracht. Zuerst die durch Satz 2. 7 nahegelegte

Definition. *Sind α, β Kreise durch den Punkt p und sind γ, δ Kreise durch den Punkt q, so sei $(\alpha\beta; p) = (\gamma\delta; q)$ im Falle $\beta \in \alpha_p$ genau dann gesetzt, wenn $\delta \in \gamma_q$ ist, und im Falle $\beta \notin \alpha_p$ genau dann, wenn es eine Abbildung $\tau \in T$ mit $(\alpha, \beta, p)^\tau = (\gamma, \delta, q)$ gibt.*

2. 8. 1. *Es gelten die Winkelaxiome* (I), (II).

Beweis. Der Beweis von (II) liegt auf der Hand. Zu (I): $(\alpha\beta; p) = (\alpha\beta; p)$ ist für $\beta \in \alpha_p$ trivial; im Falle $\beta \notin \alpha_p$ wird die Gleichung durch $(\alpha, \beta, p)^v = (\alpha, \beta, p)$ bewiesen, v die Identität von T. Sei $(\alpha\beta; p) = (\gamma\delta; q)$ und $(\alpha\beta; p) = (\varepsilon\zeta; r)$. Gilt $\beta \in \alpha_p$, so folgt $\delta \in \gamma_q$ und $\zeta \in \varepsilon_r$ und damit $(\gamma\delta; q) = (\varepsilon\zeta; r)$. Im Falle $\beta \notin \alpha_p$ gibt es also Abbildungen $\tau_1, \tau_2 \in T$ mit $(\alpha, \beta, p)^{\tau_1} = (\gamma, \delta, q)$ und $(\alpha, \beta, p)^{\tau_2} = (\varepsilon, \zeta, r)$; sicherlich ist dann $\delta \notin \gamma_q$ und $\zeta \notin \varepsilon_r$. Jetzt folgt alles aus $(\gamma, \delta, q)^{\tau_1^{-1}\tau_2} = (\varepsilon, \zeta, r)$ und aus $\tau_1^{-1}\tau_2 \in T$.

2. 8. 2. *Es seien α, β Kreise durch den Punkt p und es sei γ ein Kreis durch den Punkt q. Dann besitzt $(\alpha\beta; p) = (\gamma\xi; q)$ genau die Kreise ξ eines Berührbüschels durch q als Lösungen.*

Beweis. Im Falle $\beta \in \alpha_p$ ist die Behauptung trivial, da dann $(\alpha\beta; p) = (\gamma\xi; q)$ gleichbedeutend ist mit $\xi \in \gamma_q$. Sei $\beta \notin \alpha_p$. Es gibt dann also einen Punkt $\bar{p} \neq p$ mit $\alpha \cap \beta = \{p, \bar{p}\}$. Sei r ein Punkt auf γ, der von q verschieden ist. Seien weiter a, c Punkte mit $a \in \alpha - \{p, \bar{p}\}$, $c \in \gamma - \{q, r\}$. Ist jetzt τ die Abbildung aus T mit $(p, \bar{p}, a)^\tau = (q, r, c)$, so gilt $(\alpha\beta; p) = (\gamma\beta^\tau; q)$ mit $\beta^\tau \notin \gamma_q$. Wir behaupten: Genau die Kreise des Kontaktelements β_q^τ sind die Lösungen ξ von $(\alpha\beta; p) = (\gamma\xi; q)$. Ist nämlich ξ eine Lösung, so hat man $(\gamma\beta^\tau; q) = (\gamma\xi; q)$ wegen 2. 8, 1. — Es gibt also dann eine Abbildung $\sigma \in T$ mit $(\gamma, \beta^\tau, q)^\sigma = (\gamma, \xi, q)$. Aus (T 2) folgt aber hieraus $\xi = (\beta^\tau)^\sigma \in \beta_q^\tau$. Ist umgekehrt $\xi \neq \beta^\tau$ ein Kreis des Kontaktelementes β_q^τ, der γ in q, s schneidet — es ist $s \neq q, r$ —, so sei $\varrho \in T$ diejenige Abbildung mit $(q, r, s)^\varrho = (q, s, r)$. Man hat dann $(\gamma, q)^\varrho = (\gamma, q)$ und hiermit $(\beta^\tau)^\varrho \in \beta_q^\tau$ wegen (T 2). Wegen $s \in (\beta^\tau)^\varrho$ ist also $\xi = (\beta^\tau)^\varrho$ und wegen $(\gamma\beta^\tau; q) = (\gamma^\varrho\beta^{\tau\varrho}; q^\varrho) = (\gamma\beta^{\tau\varrho}; q)$ ist $(\alpha\beta; p) = (\gamma\beta^\tau; q) = (\gamma\xi; q)$.

2. 8. 3. *Es gilt das Winkelaxiom* (IV) *in der stärkeren Fassung: Es seien p, q, r verschiedene Punkte und ebenso p', q', r'. Es seien ferner $x_1, \ldots, x_4$ und $x_1', \ldots, x_4'$ je vier unter sich verschiedene Punkte mit*

(a) $x_i \notin (pqr) - \{p, q, r\}$, $x_i' \notin (p'q'r') - \{p', q', r'\}$ *für* $i = 1, 2, 3, 4$.

(b) *Für* $x_i =$ *resp.* p, q, r *ist* $x_i' =$ *resp.* p', q', r'.

(c) *Im Falle* $x_i \notin \{p, q, r\}$ *ist* $x_i' \notin \{p', q', r'\}$ *und weiter*

$$((pqr)\,(pqx_i);\, q) = ((p'q'r')\,(p'q'x_i');\, q'),$$
$$((prq)\,(prx_i);\, r) = ((p'r'q')\,(p'r'x_i');\, r').$$

Dann gilt $((x_1x_2x_3)\,(x_1x_2x_4);\, x_1) = ((x_1'x_2'x_3')\,(x_1'x_2'x_4');\, x_1')$.

[11]) Die Eigenschaft (T 2) kann auf Grund von Satz 3. 1 durch das Axiom von Süss ersetzt werden.

Beweis. Sei τ die Abbildung aus T mit $(p, q, r)^\tau = (p', q', r')$. Wir behaupten $x_i' = x_i^\tau$, $i = 1, 2, 3, 4$. Dies ist klar für $x_i \in \{p, q, r\}$. Sei $x_i \notin \{p, q, r\}$. Dann trifft der Fall (c) zu. Es ist aber auch wegen $\tau \in T$

$$((pqr)\,(pqx_i);\, q) = ((p'q'r')\,(p'q'x_i^\tau);\, q'),$$
$$((prq)\,(prx_i);\, r) = ((p'r'q')\,(p'r'x_i^\tau);\, r'),$$

was mit (c) und 2. 8. 1, 2. 8. 2 auf $(p'q'x_i') = (p'q'x_i^\tau)$ und $(p'r'x_i') = (p'r'x_i^\tau)$ führt. Wegen $(p'q'x_i') \neq (p'r'x_i')$ (dies folgt aus $x_i' \notin (p'q'r')$) ergibt sich hiermit

$$\{p', x_i'\} = (p'q'x_i') \cap (p'r'x_i') = (p'q'x_i^\tau) \cap (p'r'x_i^\tau) \supseteqq \{p', x_i^\tau\},$$

d. h. $x_i' = x_i^\tau$. Da $\tau \in T$ ist, hat man schließlich

$$((x_1x_2x_3)\,(x_1x_2x_4);\, x_1)) = ((x_1^\tau x_2^\tau x_3^\tau)\,(x_1^\tau x_2^\tau x_4^\tau);\, x_1^\tau) = ((x_1'x_2'x_3')\,(x_1'x_2'x_4');\, x_1').$$

2. 8. 4. $T(\Sigma) \cong T$.

Beweis. Ist $\tau(\Sigma)$ die Abbildung aus $T(\Sigma)$, die die verschiedenen Punkte a, b, c in a', b', c' überführt und ist τ die Abbildung aus T mit der gleichen Eigenschaft, so gilt $x^\tau = x^{\tau(\Sigma)}$ für alle Punkte x: Beide Abbildungen erhalten nämlich freie Winkel und daher ist

$$((a'b'c')\,(a'b'x^{\tau(\Sigma)});\, a') = ((abc)\,(abx);\, a) = ((a'b'c')\,(a'b'x);\, a'),$$
$$((a'b'c')\,(a'c'x^{\tau(\Sigma)});\, a') = ((acb)\,(acx);\, a) = ((a'c'b')\,(a'c'x);\, a'),$$

was auf $(a'b'x^{\tau(\Sigma)}) = (a'b'x^\tau)$ und $(a'c'x^{\tau(\Sigma)}) = (a'c'x^\tau)$ führt. Für jeden Punkt $x \notin (abc)$ ist demnach $x^\tau = x^{\tau(\Sigma)}$. Liegt x auf (abc), so führe man die Betrachtung für Punkte a, b, d und a', b', d' mit $d \notin (abc)$ (es ist dann ja $d^\tau = d^{\tau(\Sigma)}$) durch. Wir identifizieren τ und $\tau(\Sigma)$. Da T aus kreiswinkeltreuen Kreisverwandtschaften besteht und da $T(\Sigma)$ die Menge aller kreiswinkeltreuen Kreisverwandtschaften von Σ darstellt, so ist $T \subseteqq T(\Sigma)$. Eine Abbildung aus $T(\Sigma) - T$ überführe nun die verschiedenen Punkte a, b, c in a', b', c'. Dann muß sie also auch in T liegen, da T ebenfalls eine Abbildung enthält, die dies leistet.

Damit ist Satz 2. 8 bewiesen.

§ 3. Das Axiom von Süss und die Eigenschaft (T 2). Über Unabhängigkeitsfragen. Erweiterung gewisser affiner Ebenen zu $[M]$-Ebenen.

Für die Sätze 3. 1, 3. 2 dieses Paragraphen legen wir eine $[M]$-Ebene zugrunde mit einer Winkelvergleichung in der Stärke (I) bis (IV).

Ist φ ein freier Winkel, ist p ein vorgegebener Punkt und γ ein vorgegebener Kreis durch p, dann gibt es nach 2. 8. 2 Kreise ξ mit $(\gamma\xi;\, p) \in \varphi$.

Definition. *Es seien φ und ψ freie Winkel, p ein vorgegebener Punkt und $\alpha \ni p$ ein vorgegebener Kreis. Ist dann β ein Kreis durch p mit $(\alpha\beta;\, p) \in \varphi$ und ist γ ein Kreis durch p mit $(\beta\gamma;\, p) \in \psi$, so sei $\varphi + \psi$ gleich der Winkelklasse gesetzt, die $(\alpha\gamma;\, p)$ enthält.*

Daß die Winkeladdition unabhängig von den Repräsentanten p, α, β, γ ist, zeigen die folgenden (für $p' = p$ durch die Hilfssätze 2. 6, 2. 8 bereits bewiesenen) Hilfssätze 3. 1. 1 und 3. 1. 2.

Hilfssatz 3. 1. 1. *Sind α, β Kreise durch den Punkt p, sind α', β' Kreise durch den Punkt p' und gilt $(\alpha\beta;\, p) = (\alpha'\beta';\, p')$, so folgt $(\beta\alpha;\, p) = (\beta'\alpha';\, p')$.*

Beweis. Ist $\beta \in \alpha_p$, so ist also auch $\beta' \in \alpha_p'$, was $\alpha \in \beta_p$ und $\alpha' \in \beta_{p'}'$ impliziert. Im Falle $\beta \notin \alpha_p$ gibt es ein $\tau \in T(\Sigma)$ mit $(\alpha, \beta, p)^\tau = (\alpha', \beta', p')$. Dies ergibt aber sofort die Behauptung.

Hilfssatz 3. 1. 2. *Es seien α, β, γ Kreise durch den Punkt p, es seien α', β', γ' Kreise durch den Punkt p' und es gelte $(\alpha\beta; p) = (\alpha'\beta'; p')$, $(\beta\gamma; p) = (\beta'\gamma'; p')$. Dann folgt $(\gamma\alpha; p) = (\gamma'\alpha'; p')$.*

Beweis. Ist $\beta \in \alpha_p$ und also auch $\beta' \in \alpha'_{p'}$, so gilt wegen 2. 8. 2 und unter Benutzung von Hilfssatz 3. 1. 1

$$(\gamma\alpha; p) = (\gamma\beta; p) = (\gamma'\beta'; p') = (\gamma'\alpha'; p').$$

Ist $\gamma \in \beta_p$ und also auch $\gamma' \in \beta'_{p'}$, so gilt

$$(\alpha\gamma; p) = (\alpha\beta; p) = (\alpha'\beta'; p') = (\alpha'\gamma'; p'),$$

was auch für diesen Fall die Behauptung ergibt.

Sei nun $\beta \notin \alpha_p$, $\gamma \notin \beta_p$ und damit $\beta' \notin \alpha'_{p'}$, $\gamma' \notin \beta'_{p'}$. Dann gibt es Punkte $q \neq p$ und $q' \neq p'$ mit $\alpha \cap \beta = \{p, q\}$ und $\alpha' \cap \beta' = \{p', q'\}$. Seien $\bar{\gamma}, \bar{\gamma}'$ die durch $q \in \bar{\gamma} \in \gamma_p$ und $q' \in \bar{\gamma}' \in \gamma'_{p'}$ eindeutig bestimmten Kreise. Es gilt $(\alpha\beta; p) = (\alpha'\beta'; p')$, $(\beta\bar{\gamma}; p) = (\beta'\bar{\gamma}'; p')$ und $\beta \cap \bar{\gamma} = \{p, q\}$, $\beta' \cap \bar{\gamma}' = \{p', q'\}$, letzteres wegen $\gamma \notin \beta_p$ und $\gamma' \notin \beta'_{p'}$. Es seien nun a, a' Punkte mit $a \in \alpha - \{p, q\}$ und $a' \in \alpha' - \{p', q'\}$; es sei ferner $\tau \in T(\Sigma)$ die Abbildung mit $(p, q, a)^\tau = (p', q', a')$. Dann ist also $(\alpha\beta; p) = (\alpha'\beta^\tau; p')$ und damit $\beta^\tau \in \beta'_{p'}$; wegen $\beta^\tau \cap \beta' > \{p', q'\}$ ist weiter $\beta^\tau = \beta'$. Sei jetzt b ein Punkt mit $b \in \beta - \{p, q\}$ und sei $b' = b^\tau$. Offenbar gilt dann $b' = b^\tau \in \beta^\tau - \{p^\tau, q^\tau\} = \beta' - \{p', q'\}$ und wegen $(p, q, b)^\tau = (p', q', b')$ ist weiter $(\beta\bar{\gamma}; p) = (\beta'\bar{\gamma}^\tau; p')$; damit hat man $\bar{\gamma}^\tau \in \bar{\gamma}'_{p'}$ bzw. wegen $\bar{\gamma}^\tau \cap \bar{\gamma}' > \{p', q'\}$ sogar $\bar{\gamma}^\tau = \bar{\gamma}'$. Zusammenfassend können wir schreiben:

$$(*) \qquad (p, q, \alpha, \beta, \bar{\gamma})^\tau = (p', q', \alpha', \beta', \bar{\gamma}').$$

Hieraus folgt: Ist $\bar{\gamma} \in \alpha_p$, so ist auch $\bar{\gamma}' \in \alpha'_{p'}$; damit gilt $(\alpha\bar{\gamma}; p) = (\alpha'\bar{\gamma}'; p')$, was auf $(\alpha\gamma; p) = (\alpha'\gamma'; p')$ führt und wegen Hilfssatz 3. 1. 1 die Behauptung für diesen Sonderfall bedeutet. — Ist $\bar{\gamma} \notin \alpha_p$, so ist $\bar{\gamma}' \notin \alpha'_{p'}$. Mit (*) hat man $(\alpha\bar{\gamma}; p) = (\alpha'\bar{\gamma}'; p')$ und hiermit $(\alpha\gamma; p) = (\alpha'\gamma'; p')$ nach 2. 8. 2, was nach Hilfssatz 3. 1. 1 die Behauptung ergibt.

Die freien Winkel werden vermittels der Verknüpfung „+" zu einer Gruppe $\mathfrak{W}$ zusammengefaßt. Das neutrale Element dieser Gruppe ist der Nullwinkel. Das inverse Element $-\chi$ von χ ist durch die Klasse, die $(\beta\alpha; p)$ enthält, gegeben, wenn $(\alpha\beta; p) \in \chi$ ist: Aus $\chi = (\alpha\beta; p)$ folgt $-\chi = (\beta\alpha; p)$.

Wir zeigen jetzt, daß die Eigenschaft (T 2) zum Axiom von Süss äquivalent ist, wenn man über die folgende (gegenüber (T 1) schwächere) Eigenschaft verfügt:

(T 1)* *Sind a, b, c und a', b', c' je drei verschiedene Punkte, so gibt es mindestens eine Abbildung $\tau \in T$ mit $(a, b, c)^\tau = (a', b', c')$.*

Satz 3. 1. *Ist Σ eine $[M]$-Ebene, die eine auf den Punkten dreifach transitive Gruppe T von Kreisverwandtschaften besitzt, so sind die folgenden Aussagen äquivalent:*

(1) (T 2),

(2) *Axiom von Süss,*

(3) (*Abgeschwächtes Axiom von Süss*). *Sind $\varkappa, \varkappa'$ verschiedene Kreise durch die verschiedenen Punkte s, a, so führt jede T-Abbildung, welche $\varkappa$ in sich selbst überführt und dabei die Punkte s und a einzeln festläßt, auch $\varkappa'$ in sich selbst über.*

(4) *Es gibt einen Kreis $\varkappa_0$ und verschiedene Punkte s_0, a_0 auf $\varkappa_0$ dergestalt, daß für jeden Kreis $\varkappa'$ und für jede Abbildung $\tau \in T$ mit $s_0, a_0 \in \varkappa' \neq \varkappa_0$, $(\varkappa_0, s_0, a_0)^\tau = (\varkappa_0, s_0, a_0)$ stets $\varkappa'^\tau = \varkappa'$ ist.*

Beweis. Auf Grund von Satz 2. 2 folgt aus (1) die Aussage (2). Aus (2) folgt sicherlich (3) und aus (3) gewiß (4). Sei umgekehrt (4) erfüllt. Dann kann man (4) leicht vermittels

der Eigenschaft (T 1)* zu (3) erweitern: Sind nämlich $\varkappa$, $\varkappa'$ verschiedene Kreise durch die verschiedenen Punkte s, a und ist $\tau \in T$ eine Abbildung mit $(\varkappa, s, a)^\tau = (\varkappa, s, a)$, so betrachte man eine Abbildung $\sigma \in T$ mit $(\varkappa, s, a)^\sigma = (\varkappa_0, s_0, a_0)$. Der Kreis $\varkappa'$ geht dann in $\varkappa'^\sigma$ über. Wegen $(\varkappa, s, a)^{\tau\sigma} = (\varkappa, s, a)^\sigma = (\varkappa_0, s_0, a_0)$ ist nun $(\varkappa_0, s_0, a_0)^{\sigma^{-1}\tau\sigma} = (\varkappa_0, s_0, a_0)$. Wegen (4) ist also $(\varkappa'^\sigma)^{\sigma^{-1}\tau\sigma} = \varkappa'^\sigma$, d. h. $\varkappa'^\tau = \varkappa$.

Aus (3) folgt (2) (vgl. die Fassung von Satz 2. 2): Sei α der Kreis durch a mit $\alpha \in \varkappa_s$. Dann ist $\alpha^\tau = \alpha$. Im Falle $\alpha = \varkappa$ folgt dies aus $\alpha^\tau = \varkappa^\tau = \varkappa = \alpha$; im Falle $\alpha \cap \varkappa = s$ ist $\alpha^\tau \cap \varkappa \equiv \alpha^\tau \cap \varkappa^\tau = s^\tau \equiv s$ und also $a \equiv a^\tau \in \alpha^\tau \in \varkappa_s$, d. h. es ist ebenfalls $\alpha^\tau = \alpha$. Wir können $\varkappa' \neq \alpha$ voraussetzen, da sonst $\varkappa'^\tau = \alpha^\tau = \alpha = \varkappa'$ ist. Wir wenden dann (3) an auf α als Grundkreis, der die Fixpunkte $s^\tau = s$, $a^\tau = a$ enthält. Wegen $\varkappa' \neq \alpha$ und $s, a \in \varkappa'$ ist damit tatsächlich $\varkappa'^\tau = \varkappa$.

Aus (2) folgt (1): Seien also α, β Kreise durch einen Punkt p und sei τ eine Abbildung aus T mit $(\alpha, p)^\tau = (\alpha, p)$. Dann ist $\beta^\tau \in \beta_p$ nachzuweisen. Dies ist klar im Falle $\beta \in \alpha_p$, denn dann ist $\beta^\tau \in \alpha_p^{\tau}{}^\tau = \alpha_p = \beta_p$. Sei also $\beta \cap \alpha = \{p, r\}$, $r \neq p$. Im Gegensatz zur Behauptung sei jetzt $\beta^\tau \cap \beta = \{p, q\}$, $q \neq p$, angenommen. Es ist $q \notin \alpha$: Im Falle $q \neq r$ hätte man sonst $\beta = (pqr) = \alpha$. Im Falle $q = r$ wäre $\{p, r\} = \beta \cap \alpha = \beta^\tau \cap \beta$, d. h. $\{p, r\} = \alpha \cap \beta^\tau$ wegen $\beta^\tau \neq \alpha^\tau = \alpha$; man hätte daher $r^\tau = r$ auf Grund von $\{p, r\} = \alpha \cap \beta^\tau = \alpha^\tau \cap \beta^\tau = \{p^\tau, r^\tau\}$. Mit (3) — angewandt auf den Grundkreis α und die Fixpunkte p, r — ergäbe sich dann $\beta^\tau = \beta$ entgegen der Annahme. — Mit s bezeichnen wir den Punkt r^τ; es ist also $\alpha \cap \beta^\tau = \{p, s\}$. Es sei nun σ eine Abbildung aus T mit $(p, q, r)^\sigma = (p, q, s)$. Wir haben dann $(\beta, p, r)^{\tau^{\sigma-1}} = (\beta, p, r)$. Nun ergibt (3) aber $\alpha^{\tau\sigma^{-1}} = \alpha$. Hieraus folgt $\alpha^\sigma = \alpha^\tau = \alpha$. Wir wenden jetzt (2) an auf α als Grundkreis und auf die Abbildung $\sigma \in T$ mit den Fixpunkten p, q; (2) ergibt $\beta^\sigma = \beta$. Da aber $\beta^{\tau\sigma^{-1}} = \beta$ war, folgt $\beta = \beta^\sigma = \beta^\tau$ im Widerspruch zu $\beta \cap \beta^\tau = \{p, q\}$.

Satz 3. 2. *Gegeben sei eine [H]-Kreisebene Σ, in der nicht alle Punkte auf einem einzigen Kreise liegen, und weiterhin eine Gruppe T von Kreisverwandtschaften von Σ mit den Eigenschaften:*

(T 1)* *Sind a, b, c und a', b', c' je drei verschiedene Punkte, so gibt es wenigstens eine Abbildung τ aus T mit $(a, b, c)^\tau = (a', b', c')$.*

(2) *Abgeschwächtes Axiom von Süss (Eigenschaft* (3) *in Satz* 3. 1).

Dann gilt (T 1)* *in der schärferen Fassung* (T 1).

Beweis. Es seien p, q, r verschiedene Punkte. Dann zeigen wir, daß eine Abbildung $\tau \in T$ mit $(p, q, r)^\tau = (p, q, r)$ die Identität sein muß. Der Kreis durch die Punkte p, q, r sei mit α bezeichnet. Wegen $(\alpha, p, q, r)^\tau = (\alpha, p, q, r)$ bleibt nach (2) jeder Kreis durch p, q und auch jeder Kreis durch p, r gegenüber τ fest. Ist nun z ein Punkt $\notin \alpha$, so ist

$$\{p, z\} = (pqz) \cap (prz) = (pqz)^\tau \cap (prz)^\tau = \{p, z^\tau\},$$

d. h. es ist $z^\tau = z$. Nach Voraussetzung können nicht alle Punkte von Σ auf α liegen. Es gibt also einen Punkt $z \notin \alpha$. Führen wir nun die gleiche Betrachtung für die Punkte p, q, z durch, die für p, q, r vorgenommen wurde, so erkennt man, daß auch jeder Punkt von α gegenüber τ festbleibt. τ ist also die Identität.

In den von v. d. Waerden und Smid begründeten Geometrien läßt sich ein Winkelbegriff einführen, der den Eigenschaften (I) *bis* (IV) *genügt und weiterhin*

(a) *dem Peripheriewinkelsatz,*

(b) *dem Satz über den Sehnentangentenwinkel,*

(c) *der Eigenschaft* $(\alpha\beta; p) = (\beta\alpha; q)$ *für* $\alpha \cap \beta > \{p, q\}$, $p \neq q$.

Wir wollen zeigen, daß jede der Eigenschaften (a), (b), (c) für sich — zu den Eigenschaften (I) bis (IV) hinzugenommen — ergibt, daß $\mathfrak{W}$ abelsch ist. Indem wir später eine $[M]$-Ebene angeben mit Gültigkeit der Winkeleigenschaften (I) bis (IV), in der $\mathfrak{W}$ nichtabelsch ist, werden wir darauf geführt, daß keine der Eigenschaften (a), (b), (c) aus den Axiomen (I) bis (IV) hergeleitet werden kann.

Satz 3. 3. *Es sei Σ eine $[M]$-Ebene, in der eine Winkelvergleichung in der Stärke* (I) *bis* (IV) *gegeben ist. Dann impliziert jede der folgenden Eigenschaften die Kommutativität von $\mathfrak{W}$:*

(a) *Es seien a, b, c, d verschiedene Punkte eines Kreises $\varkappa$ und es sei w ein nicht auf $\varkappa$ gelegener Punkt. Dann gilt $((wcb)\,(wca);\,c) = ((wdb)\,(wda);\,d)$.*

(b) *Es seien a, b, c, d nicht gemeinsam auf einem Kreise gelegene Punkte. Dann gilt*

$$((abc)\,(abd);\,a) = ((dcb)\,(dca);\,d).$$

(c) *Es seien α, β Kreise durch die verschiedenen Punkte p, q. Dann gilt*

$$(\alpha\beta;\,p) = (\beta\alpha;\,q).$$

Beweis. Wir zeigen, daß (b) aus (a) folgt, (c) aus (b) und aus (c) die Kommutativität von $\mathfrak{W}$.

(a) *impliziert* (b): Seien also a, b, c, d nicht gemeinsam auf einem Kreise gelegene Punkte. Dann konstruieren wir den Kreis ξ durch b, d mit $((abc)\,(abd);\,a) = ((dcb)\,\xi;\,d)$. Berührt ξ den Kreis (acd) in d, so sind wir fertig. Wegen $\xi \neq (acd)$ können wir also annehmen $\xi \notin (acd)_d$, was zum Widerspruch geführt werden soll. Sei $\xi \cap (acd) = \{d, a'\}$, $a' \neq d$. Es ist a' auch $\neq c$, da sonst $\xi = (bdc)$, d.h. da sonst $0 = ((dcb)\,\xi;\,d) = ((abc)\,(abd);\,a)$ sein müßte. Wir konstruieren noch den Kreis $(a'cb)$. Dann ist also mit Hilfe von (a):

$$((a'bc)\,\xi;\,a') = ((abc)\,(abd);\,a) = ((dcb)\,\xi;\,d).$$

Da $(a'bc)$, ξ Kreise durch die verschiedenen Punkte a', b sind und (dcb), ξ Kreise durch die verschiedenen Punkte d, b, so haben wir $((a'bc)\,\xi;\,b) = ((dcb)\,\xi;\,b)$ nach Hilfssatz 2. 5 bzw. $(\xi(a'bc);\,b) = (\xi(dcb);\,b)$ nach Hilfssatz 2. 6. Axiom (III) ergibt nun $(a'bc) = (dcb)$, d. h. $a' \in (dcb) \cap (acd) = \{c, d\}$, was bereits ausgeschlossen wurde.

(b) *impliziert* (c): Für $\alpha = \beta$ ist die Aussage (c) trivial. Sei also $\alpha \neq \beta$. Es sei a ein Punkt auf α, der nicht auf β liegt; sei ferner b ein Punkt mit $b \in \beta - \alpha$. Auf Grund von (b) gilt dann: $((bap)\,(baq);\,a) = ((qpa)\,(qpb);\,p)$. Weiterhin gilt mit (b) auch $((abp)\,(abq);\,a) = ((qpb)\,(qpa);\,q)$, was zusammengefaßt $((qpa)\,(qpb);\,p) = ((qpb)\,(qpa);\,q)$, d. h. die Behauptung ergibt.

Aus (c) *folgt die Kommutativität von $\mathfrak{W}$*: Seien φ, ψ beliebige Elemente von $\mathfrak{W}$. Wir können $\varphi \neq 0$ und $\psi \neq 0$ annehmen, da sonst $\varphi + \psi = \psi + \varphi$ trivial ist. Seien α, β verschiedene Kreise durch die verschiedenen Punkte p, q mit $\varphi = (\alpha\beta;\,p)$ und seien β, γ verschiedene Kreise durch p, q mit $\psi = (\beta\gamma;\,p)$. Dann ist also $\varphi + \psi = (\alpha\gamma;\,p)$. Mit (c) gilt weiterhin

$$\psi + \varphi = (\gamma\beta;\,q) + (\beta\alpha;\,q) = (\gamma\alpha;\,q) = (\alpha\gamma;\,p) = \varphi + \psi.$$

Wie in [16] gezeigt, bilden die von einem festen Punkt w verschiedenen Punkte und die Kreise durch w (als Geraden aufgefaßt) eine affine Ebene. Es gilt

Satz 3. 4. *Ist Σ eine $[M]$-Ebene mit einer Winkelvergleichung in der Stärke* (I) *bis* (IV), *so gilt in der aus Σ durch Auswahl eines beliebigen Punktes w entspringenden affinen Ebene $E(\Sigma;\,w)$ der Satz von Desargues*[12]).

[12]) Unser Beweis dieses Satzes macht ausgiebig Gebrauch von der Eigenschaft (T 2).

Beweis. Wir zeigen die beiden folgenden Eigenschaften, die bekanntlich[13]) den Satz von Desargues implizieren:

1) Sind p, q von w verschiedene Punkte, so gibt es eine Translation in $E(\Sigma; w)$, die p in q überführt.

2) Gegeben seien drei untereinander und von w verschiedene Punkte p, q, r derart, daß w, p, q, r konzyklisch ist. Dann gibt es eine Dilatation in $E(\Sigma; w)$, die p festläßt und die q in r überführt.

Zu 1): Wir können $p \neq q$ voraussetzen. Ist dann r ein nicht auf (pqw) gelegener Punkt und ist ξ der durch r gehende, (pqw) in w berührende Kreis — also die Parallele durch r zur „Geraden" (pq) in $E(\Sigma; w)$ —, so sei unter s derjenige Punkt $\neq w$ von ξ verstanden, der auch auf der Parallelen η zu (rp) durch q gelegen ist. Ein solcher Punkt s existiert, da sonst $q \in \eta \in \xi_w$, d. h. $\eta = (pqw)$ sein müßte, was wegen $\eta \in (rpw)_w$ auf $r \in (pqw)$ führte. Man hat $s \neq r$. Es sei dann τ diejenige Abbildung aus $T(\Sigma)$, für die $(w, p, r)^\tau = (w, q, s)$ ist. τ ist Translation in $E(\Sigma; w)$, die also p nach q überführt: Man hat $(wpq)^\tau = (wpq)$. Es ist nämlich $\big((wpr)\,(wpq); w\big) = \big((wqs)\,(wpq)^\tau; w\big)$ wegen $\tau \in T(\Sigma)$; da aber auf Grund von $\eta \in (wpr)_w$ auch $\big((wpr)\,(wpq); w\big) = \big(wqs)\,(wpq); w\big)$ ist, gilt $(wpq)^\tau \in (wpq)_w$, d. h. $(wpq)^\tau = (wpq)$ wegen $w, q \in (wpq)^\tau \cap (wpq)$. — Für einen beliebigen Punkt $t \neq w$ ist $t \neq t^\tau$ und weiter $(wtt^\tau)^\tau = (wtt^\tau)$. Dies ist für $t = p$ klar. Sei $t \neq p$. Wegen $(wpq)^\tau = (wpq)$ und $w^\tau = w$ ist $(wpt)^\tau \in (wpt)_w$ nach (T 2). Im Falle $t^\tau = t$ wäre also $(wqt) = (wpt)$, d. h. $t \in (wpq)$; setzt man in (T 2) wiederum $\alpha = (wpq)$, den dort benutzten Punkt p hier gleich w und $\beta = (wtr)$, so wäre also $(wtr)^\tau \in (twr)_w$, d. h. $(wts) = (wtr)$, d. h. $t \in (wrs)$, was $t \in (wpq) \cap (wrs) = \{w\}$ ergäbe. Weiterhin erkennt man mit Hilfe von (T 2) auch $(wtt^\tau)^\tau \in (wtt^\tau)_w$; wegen $w, t^\tau \in (wtt^\tau)^\tau \cap (wtt^\tau)$ ist also $(wtt^\tau)^\tau = (wtt^\tau)$.

Sind u, v verschiedene Punkte $\neq w$ und ist μ der Kreis mit $u^\tau \in \mu \in (wuv)_w$, so gilt $v^\tau \in \mu$: Setzen wir $\alpha = (wuu^\tau)$, $\beta = (wuv)$ in (T 2) und den dort benutzten Punkt p hier gleich w, so kommt $(wu^\tau v^\tau) \equiv \beta^\tau \in \beta_w = (wuv)_w$. Es ist also $\mu = (wu^\tau v^\tau)$ und damit $v^\tau \in \mu$.

Zu 2): τ sei die Abbildung aus $T(\Sigma)$, für die $(w, p, q)^\tau = (w, p, r)$ ist. τ ist Dilatation in $E(\Sigma; w)$, die also die gewünschten Eigenschaften hat: Ist u ein Punkt $\neq p, w$, so ist $u^\tau \neq u$, da sonst τ drei Fixpunkte hätte, was $\tau = v$, d. h. $q = r$ bedeutete. Es ist $u^\tau \in (wpu)$ für $u \neq w, p$; dies folgt aus $\big((wpq)\,(wpu); p\big) = \big((wpr)\,(wpu^\tau); p\big) = \big((wpq)\,(wpu^\tau); p\big)$. — Sind u, v verschiedene Punkte $\neq w$ und ist μ der Kreis mit $u^\tau \in \mu \in (wuv)_w$, so gilt $v^\tau \in \mu$: Dies wird im Falle $u \neq p$ wörtlich wie unter 1) über (T 2) bewiesen.

Der nun folgende Satz sagt über die Erweiterung von affinen Ebenen zu $[M]$-Ebenen aus.

Satz 3. 5. *Π sei eine affine Ebene, $\mathfrak{g}$ sei eine fest ausgewählte Gerade von Π und $0, 1$ seien fest ausgewählte verschiedene Punkte von $\mathfrak{g}$. Zur Menge $\mathfrak{p}$ der Punkte von Π fügen wir einen neuen Punkt ∞ hinzu; wir schreiben $\mathfrak{P} = \mathfrak{p} \cup \{\infty\}$. Der Punkt ∞ soll zu jeder Geraden hinzuadjungiert werden; ist eine beliebige Gerade (etwa $\mathfrak{a}$) gegeben, so bezeichnen wir die aus der Geraden durch Hinzufügung des Punktes ∞ entstehende neue Punktmenge (hier $\mathfrak{a} \cup \{\infty\}$) — soweit einfach möglich — durch den entsprechenden kleinen griechischen Buchstaben (hier α); insbesondere ersetzen wir $\mathfrak{g} \cup \{\infty\}$ durch γ.*

Es sei ferner T eine Gruppe von eineindeutigen Abbildungen von $\mathfrak{P}$ auf sich mit den Eigenschaften:

(*) Sind a, b, c verschiedene Punkte aus $\mathfrak{P}$, ebenso a', b', c', dann gibt es mindestens eine Abbildung $\tau \in T$ mit $a^\tau = a'$, $b^\tau = b'$, $c^\tau = c'$.

[13]) Siehe E. Artin [1], S. 58ff. — Übrigens ergibt Axion (IV) in Verbindung mit Hilfssatz 2. 5 und Axion (III) a) ebenfalls den affinen Satz von Desargues in $E(\Sigma; w)$, der ja den Desarguesschen Satz zur Folge hat.

(**) *Ist* $\mathfrak{l}$ *eine Gerade, ist* τ *eine Abbildung aus* T *mit* $\infty^\tau = \infty$ *und* $\infty^\tau, 0^\tau, 1^\tau \in \lambda \equiv \mathfrak{l} \cup \{\infty\}$, *dann folgt* $\gamma^\tau = \lambda$.

(***) *Ist* τ *eine Abbildung aus* T *mit* $\infty^\tau, 0^\tau, 1^\tau \in \gamma$, *dann folgt* $\gamma^\tau = \gamma$.

Definiert man jetzt eine Kreisebene Σ *dadurch, daß man die Punktmengen* γ^τ, $\tau \in T$, *als Kreise auszeichnet, so bildet* Σ *eine* $[M]$*-Ebene, in der die um den Punkt* ∞ *vermehrten Geraden von* Π *speziell die Kreise durch* ∞ *sind. Die Abbildungen von* T *sind weiterhin Kreisverwandtschaften.*

Beweis. Zunächst zeigen wir, daß durch drei verschiedene Punkte a, b, c von $\mathfrak{P}$ genau ein Kreis geht. Ist τ eine Abbildung von T, die $\infty, 0, 1$ nacheinander in a, b, c überführt, so ist gewiß γ^τ ein Kreis mit $\gamma^\tau \ni a, b, c$. Angenommen nun, es gäbe einen Kreis $\gamma^\sigma \neq \gamma^\tau$ mit $\gamma^\sigma \ni a, b, c$. Sind u, v, w die Punkte von γ mit $u^\sigma = a$, $v^\sigma = b$, $w^\sigma = c$, so ist $\infty^{\tau\sigma^{-1}} = u$, $0^{\tau\sigma^{-1}} = v$, $1^{\tau\sigma^{-1}} = w$, was mit (***) $\gamma^{\tau\sigma^{-1}} = \gamma$ bedeutet. Also ist $\gamma^\tau = \gamma^\sigma$, entgegen der Annahme. Wir beweisen jetzt das Reichhaltigkeitsaxiom: γ ist ein Kreis wegen $\gamma = \gamma^v$, v die Identität von T. Die Gerade $\gamma - \{\infty\}$ enthält aber nicht alle Punkte der affinen Ebene Π. Ist p ein Punkt mit $p \in \mathfrak{p} - (\gamma - \{\infty\})$, dann sind $\infty, 0, 1, p$ vier verschiedene Punkte, die nicht gemeinsam einem Kreise angehören; gäbe es nämlich einen Kreis γ^ϱ mit $\gamma^\varrho \ni \infty, 0, 1, p$, so wäre wegen $\gamma \cap \gamma^\varrho \ni \infty, 0, 1$ nach dem zuerst Bewiesenen $\gamma = \gamma^\varrho$ und also doch $p \in \gamma - \{\infty\}$ wegen $p \neq \infty$. — Wegen $|\gamma| = |\gamma^\tau|$ für alle $\tau \in T$ sieht man, daß jeder Kreis wenigstens drei verschiedene Punkte besitzt.

Ist $\mathfrak{a}$ eine Gerade von Π, dann ist gewiß $\alpha \equiv \mathfrak{a} \cup \{\infty\}$ ein Kreis: Sind nämlich a_1, a_2 zwei verschiedene Punkte von $\mathfrak{a}$ und ist τ eine Abbildung aus T mit $\infty^\tau = \infty$, $0^\tau = a_1$, $1^\tau = a_2$, so ist wegen (**) das Bild $\gamma^\tau = \alpha$. Ist γ^τ ein Kreis durch ∞, so ist $\gamma^\tau - \{\infty\}$ eine Gerade: Seien ∞, r, s verschiedene Punkte von γ^τ und sei $\mathfrak{l}$ die Gerade durch r, s. Ist dann τ_1 eine Abbildung aus T mit $\infty^{\tau_1} = \infty$, $0^{\tau_1} = r$, $1^{\tau_1} = s$, so ist — da durch drei verschiedene Punkte genau ein Kreis geht — $\gamma^{\tau_1} = \gamma^\tau$. Nach (**) ist aber $\gamma^{\tau_1} = \lambda$.

Bevor wir den Berührsatz beweisen, sei gezeigt, daß jede Abbildung τ aus T eine Kreisverwandtschaft darstellt: Ist γ^τ ein Kreis, dann wird er durch eine beliebige Abbildung $\sigma \in T$ in $(\gamma^\tau)^\sigma = \gamma^{\tau\sigma}$ — also wieder in einen Kreis — überführt; ist weiterhin $p \in \mathfrak{P}$ ein Punkt mit $p \notin \gamma^\tau$, dann ist auch $p^\sigma \notin \gamma^{\tau\sigma}$, da sonst $p^\sigma = g^{\tau\sigma}$, $g \in \gamma$, und also $p = g^\tau \in \gamma^\tau$ wäre.

Zum Berührsatz! Ist γ^τ ein Kreis, sind p, q Punkte aus $\mathfrak{P}$ mit $p \in \gamma^\tau$, $q \notin \gamma^\tau$, dann gibt es genau einen Kreis γ^ϱ durch p, q, der mit γ^τ nur einen Punkt p gemeinsam hat: Da — wie bewiesen — jeder Kreis wenigstens drei verschiedene Punkte enthält, gibt es Punkte $c_1, c_2 \neq c_1$ auf γ^τ, die von p verschieden sind. Es sei τ_1 eine Abbildung aus T mit $(\infty, 0, 1)^{\tau_1} = (p, c_1, c_2)$. Dann ist $\gamma^\tau \equiv \gamma^{\tau_1}$. Durch das Urbild $q^{\tau_1^{-1}}$ von q gegenüber τ_1 geht nach dem Parallelenaxiom ein Kreis, der mit γ nur den Punkt ∞ gemeinsam hat. Ist dieser Kreis durch γ^σ gegeben, so enthält der Kreis $\gamma^{\sigma\tau_1}$ die Punkte p und q; weiterhin ist $\gamma^{\sigma\tau_1} \cap \gamma^{\tau_1} = p$. Gäbe es nämlich noch einen Punkt $r \in \gamma^{\sigma\tau_1} \cap \gamma^{\tau_1} - \{p \equiv \infty^{\tau_1}\}$, so wäre $r^{\tau_1^{-1}} \in \gamma^\sigma \cap \gamma - \{\infty\} = \emptyset$. Einen von $\gamma^{\sigma\tau_1}$ verschiedenen Kreis durch p, q, der mit γ^τ nur den Punkt p gemeinsam hat, gibt es nicht: Angenommen, γ^ϱ wäre doch ein solcher. Vermöge der Kreisverwandtschaft $\tau_1^{-1} \in T$ geht $\gamma^\tau = \gamma^{\tau_1}$ in γ über und γ^ϱ in $\gamma^{\varrho\tau_1^{-1}}$. Wegen $p \in \gamma^\varrho$ ist $\infty = p^{\tau_1^{-1}} \in \gamma^{\varrho\tau_1^{-1}}$. Daher ist $\gamma^{\varrho\tau_1^{-1}} - \{\infty\}$ eine Gerade $\mathfrak{a}$. Da $\mathfrak{a}$ aber keinen Punkt mit γ gemeinsam hat (das Abbild eines solchen Punktes gegenüber τ_1 läge nämlich auf $\gamma^{\tau_1} \cap \gamma^\varrho$) und da $q^{\tau_1^{-1}} \in \mathfrak{a}$ ist, muß $\gamma^{\varrho\tau_1^{-1}} = \mathfrak{a} \cup \{\infty\} \equiv \gamma^\sigma$ sein nach dem Parallelenaxiom in Π. Es ist also $\gamma^\varrho = \gamma^{\sigma\tau_1}$ entgegen der Annahme.

Wir geben jetzt ein Beispiel einer $[M]$-Ebene an, in der eine Winkelvergleichung (I) bis (IV) eingeführt werden kann, in der die Winkelgruppe $\mathfrak{W}$ nichtabelsch ist.

Tits [16] entnehmen wir folgendes Ergebnis: R_5 sei der Restklassenkörper mod 5. Definiert man dann auf der Menge $F = R_5 \times R_5$ der Paare von Elementen aus R_5 Addition und Multiplikation durch

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$

$$(a_1, a_2)(b_1, b_2) = \begin{cases} (a_1 b_1 - a_2 b_2,\ a_2 b_1 + (a_1 - a_2) b_2) \\ (a_1 b_1 + (a_2 - a_1) b_2,\ a_2 b_1 - a_1 b_2) \end{cases}$$

$$\text{für } a_1^2 - a_1 a_2 + a_2^2 \begin{cases} \in \{1, 4\} \\ \in \{0, 2, 3\} \end{cases},$$

so bilden die eineindeutigen Substitutionen von $F \cup \{\infty\}$ auf sich

$$y(x) = \begin{cases} ax + b & \text{für } x \in F \\ \infty & x = \infty \end{cases}$$

$$y(x) = \begin{cases} a(x + c)' + b & x \in F,\ x \neq -c \\ \infty & \text{für } x \in F,\ x = -c \\ b & x = \infty \end{cases}$$

eine minimal dreifach transitive Gruppe T auf $F \cup \{\infty\}$, wenn $a, b, c \in F$, $a \neq (0, 0)$ und

$$a' = (a_1, a_2)' = \left(\frac{a_1 - a_2}{a_1^2 - a_1 a_2 + a_2^2}, \frac{-a_2}{a_1^2 - a_1 a_2 + a_2^2} \right)$$

gesetzt ist.

F ist, wie man leicht nachprüft, ein vollständiger Fastkörper, dessen Zentrum R_5 (eigentlich $(R_5, 0)$) ist. F genügt nicht ausnahmslos dem kommutativen Gesetz der Multiplikation und auch nicht durchweg dem linksseitigen Distributivgesetz $(a + b)c = ac + bc$. $a \to a'$ ist ein involutorischer Automorphismus der multiplikativen Gruppe F^* von F, der der weiteren Bedingung $(a' + 1)' = -(a + 1)' + 1$ für $a \neq 0, -1$ genügt.

Mit diesem Resultat gehen wir in unseren Satz 3. 5 ein, indem wir dort für die Ebene Π die affine Ebene über R_5 nehmen. Die Punkte $a = (a_1, a_2)$ von Π seien mit den Elementen von F identifiziert. Unter der Geraden $\mathfrak{g}$ sei die Gerade aller Punkte $(x, 0)$, $x \in R_5$, verstanden. $0 = (0, 0)$, $1 = (1, 0)$ seien die fest ausgewählten Punkte von $\mathfrak{g}$. Wir haben also (**) und (***) nachzuweisen. Zu (**): Es sei $\mathfrak{l}$ eine Gerade und τ eine Abbildung aus T mit $\infty^\tau = \infty$ und $\infty^\tau, 0^\tau, 1^\tau \in \lambda \equiv \mathfrak{l} \cup \{\infty\}$. Wegen $\infty^\tau = \infty$ ist τ von der Form $y = ax + b$, $a \neq 0$, $a, b \in F$. Es ist also $0^\tau = b$, $1^\tau = a + b$. Die Gerade $\mathfrak{l}$ ist dann durch alle Punkte x mit $x = \chi(a + b) + (1 - \chi) b$, $\chi \in R_5$, gegeben, d. h. also durch alle Punkte $x = \chi a + b$, $\chi \in R_5$, wenn man beachtet, daß R_5 das Zentrum von F darstellt, daß also $(1 - \chi) b = b(1 - \chi) = b - b\chi = b - \chi b$ ist. Damit ist aber tatsächlich $\lambda = \gamma^\tau$. Zu (***): Sei τ eine Abbildung aus T mit $\infty^\tau, 0^\tau, 1^\tau \in \gamma$. Zu zeigen ist $\gamma^\tau = \gamma$. Wir können $\infty^\tau \neq \infty$ annehmen, da der Fall $\infty^\tau = \infty$ unter (**) bereits miterfaßt ist. Dann ist τ von der Form

$$y = \begin{cases} a(x + c)' + b & x \in F,\ x \neq -c \\ \infty & \text{für } x = -c \\ b & x = \infty \end{cases},$$

$a, b, c \in F$, $a \neq 0$. Weiter ist $\infty^\tau = b$, $0^\tau = ac' + b$ für $c \neq 0$ und $= \infty$ für $c = 0$, $1^\tau = a(1 + c)' + b$ für $c \neq -1$ und $= \infty$ für $c = -1$.

1. Fall: $c \neq 0, -1$.

Wir haben also b, $ac' + b$, $a(1 + c)' + b \in R_5$ wegen $\infty^\tau, 0^\tau, 1^\tau \in \gamma$ und $\infty \neq \infty^\tau, 0^\tau, 1^\tau$. Es ist ac', $a(1 + c)' \in R_5$ und weiter [man beachte $(c')^{-1} = (c^{-1})'$ für $c \neq 0$, da

$1 = (cc^{-1})' = c'(c^{-1})'$ ist] $(c^{-1})' a^{-1} \in R_5$, d.h. $R_5 \ni (c^{-1})' a^{-1} a(1+c)' = (c^{-1}+1)' = 1/(c^{-1}+1)$. Hieraus folgt $c^{-1} + 1 \in R_5$, d. h. $c \in R_5$. Aus $c \in R_5$ folgt $c' \in R_5$, was mit $ac' \in R_5$ auf $a \in R_5$ führt. Damit ist $a(\chi + c)' + b \in R_5$ für alle χ mit $-c \neq \chi \in R_5$.

2. Fall: $c = -1$.

Wir haben $b, -a + b \in R_5$, d. h. $a \in R_5$.

Auf Grund von Satz 3. 5 bildet also $F \cup \{\infty\}$ eine $[M]$-Ebene. Sie besitzt eine Gruppe T von Kreisverwandtschaften, die der Eigenschaft (T 1) genügt. Es gilt auch (T 2). Zum Beweise benutzen wir Satz 3. 1, indem wir die dort genannte Eigenschaft (4) für $\varkappa_0 = \gamma$, $s_0 = \infty$, $a_0 = 0$ nachweisen. Sei also $\varkappa'$ ein Kreis $\neq \gamma$ durch $\infty, 0$ und sei τ eine Abbildung aus T mit $(\gamma, \infty, 0)^\tau = (\gamma, \infty, 0)$. Wegen $\infty^\tau = \infty$ ist τ von der Form $y = ax + b$, $a \neq 0$; wegen $0^\tau = 0$ und $1^\tau \in \gamma$ auf Grund von $\gamma^\tau = \gamma$ ist nun $y = ax$, $a \in R_5$. Diese Abbildung überführt aber den Kreis $\varkappa'$, der vermittels $\{\infty, x \mid x = \varrho q,\ \varrho \in R_5\}$ (q ein von 0, ∞ verschiedener fester Punkt von $\varkappa'$) dargestellt werden kann, in sich.

Wir bestimmen die Winkelgruppe $\mathfrak{W}$ in unserem Beispiel: Sie kann nach Axiom (III) durch die Winkel $(\gamma\alpha; 0)$ repräsentiert werden, wo α alle Kreise durch 0, ∞ durchläuft. Die sechs verschiedenen Kreise γ und α_i, $i = 0, 1, 2, 3, 4$, durch 0, ∞ können in folgender Weise angegeben werden:

$$\gamma,\ \alpha_i = (\infty\ 0(i, 1)),\ i = 0, 1, 2, 3, 4.$$

Die Winkel $(\gamma\alpha; 0)$ beziehen wir nun eineindeutig auf die Elemente (1), (12), (13), (23), (123), (132) der symmetrischen Gruppe $\mathfrak{S}_3$:

$$\gamma \longleftrightarrow (1),\ \alpha_0 \longleftrightarrow (123),\ \alpha_1 \longleftrightarrow (132),\ \alpha_2 \longleftrightarrow (12),\ \alpha_3 \longleftrightarrow (13),\ \alpha_4 \longleftrightarrow (23).$$

Die Gruppe $\mathfrak{W}$ ist isomorph zur symmetrischen Gruppe $\mathfrak{S}_3$: Wir setzen

$$(\gamma\alpha_i; 0) + (\gamma\alpha_j; 0) = (\gamma\xi; 0)$$

und haben also

$$(\gamma\alpha_j; 0) = (\alpha_i\xi; 0)$$

nach ξ aufzulösen. Wir überführen dazu ∞ nach ∞, 0 nach 0 und 1 nach $(i, 1)$: $y = (i, 1)x$. Der Kreis γ geht in α_i über und α_j muß dann in ξ übergehen:

$$\alpha_j = (0\ 1\ (j, 1)) \to (0\ 1\ (i, 1)(j, 1)) \equiv \xi.$$

Es ist nun

$$\xi = \begin{cases} \gamma & \text{für } i = j \in \{2, 3, 4\} \text{ bzw. für } i, j \in \{0, 1\} \text{ mit } i \neq j \\ \alpha_{\frac{ij+1-i}{j-i}} & \text{für } i \in \{2, 3, 4\},\ j \text{ beliebig } \neq i \\ \alpha_{\frac{ij-1}{j+i-1}} & \text{für } i \in \{0, 1\},\ j \text{ beliebig } \neq 1 - i, \end{cases}$$

woraus leicht $\mathfrak{W} \cong \mathfrak{S}_3$ zu entnehmen ist (die Indizes sind mod 5 zu berechnen).

Da die Gruppe $\mathfrak{S}_3$ nichtabelsch ist, sieht man mit Satz 3. 3, daß in dem angegebenen Beispiel weder der Peripheriewinkelsatz noch der Satz über den Sehnentangentenwinkel erfüllt ist.

Wir schließen § 3 ab mit

Satz 3. 6. *Es sei Σ eine $[M]$-Ebene, in der eine Winkelvergleichung in der Stärke* (I) *bis* (IV) *gegeben ist. Dann existiert ein involutorischer Antiautomorphismus $\varphi \to \bar{\varphi}$ von $\mathfrak{W}$ auf sich derart, daß aus $(\alpha\beta;\, p) = \varphi$ stets $(\beta\alpha;\, q) = \bar{\varphi}$ für sich in verschiedenen Punkten p, q schneidende verschiedene Kreise α, β folgt.*

Beweis. Ist φ ein freier Winkel $\neq 0$, sind α_0, β_0 verschiedene Kreise durch die verschiedenen Punkte p_0, q_0 mit $(\alpha_0\beta_0;\, p_0) = \varphi$, so sei $\bar{\varphi}$ der freie Winkel mit $\bar{\varphi} = (\beta_0\alpha_0;\, q_0)$. Diese Konstruktion ist unabhängig von den speziellen Repräsentanten $\alpha_0, \beta_0, p_0, q_0$: Wir haben zu zeigen, daß aus $(\alpha_0\beta_0;\, p_0) = (\alpha\beta;\, p)$, $\alpha \cap \beta = \{p, q\}$ folgt, daß $(\beta_0\alpha_0;\, q_0) = (\beta\alpha;\, q)$ gilt. Seien zum Beweise a_0, a Punkte mit $a_0 \in \alpha_0 - \beta_0$, $a \in \alpha - \beta$, $\tau \in T(\Sigma)$ die Abbildung mit $(p_0, q_0, a_0)^\tau = (p, q, a)$. Dann folgt aus

$$(\alpha\beta;\, p) = (\alpha_0\beta_0;\, p_0) = (\alpha_0^\tau\beta_0^\tau;\, p_0^\tau) = (\alpha\beta_0^\tau;\, p)$$

zunächst $\beta_0^\tau \in \beta_p$; wegen $p, q \in \beta_0^\tau \cap \beta$ ist also $\beta_0^\tau = \beta$. Damit ist

$$(\beta_0\alpha_0;\, q_0) = (\beta_0^\tau\alpha_0^\tau;\, q_0^\tau) = (\beta\alpha;\, q).$$

Dem Nullwinkel 0 sei zugeordnet $\bar{0} = 0$. Offenbar ist $\bar{\bar{\varphi}} = \varphi$. Weiterhin ist $\varphi \to \bar{\varphi}$ eine eineindeutige Abbildung von $\mathfrak{W}$ auf sich: Jedem $\varphi \in \mathfrak{W}$ ist eindeutig ein Bild $\bar{\varphi} \in \mathfrak{W}$ zugeordnet. Sind φ_1, φ_2 verschiedene freie Winkel, so folgt $\bar{\varphi}_1 \neq \bar{\varphi}_2$; aus $\bar{\varphi}_1 = \bar{\varphi}_2$ folgte $\varphi_1 = \bar{\bar{\varphi}}_1 = \bar{\bar{\varphi}}_2 = \varphi_2$. Zu jedem freien Winkel ψ gibt es ein φ mit $\bar{\varphi} = \psi$; man setze $\varphi = \bar{\psi}$. Es gilt $\overline{\varphi + \psi} = \bar{\psi} + \bar{\varphi}$ für alle φ, ψ aus $\mathfrak{W}$. Dies ist klar für $0 \in \{\varphi, \psi\}$. Sei $\varphi \neq 0$, $\psi \neq 0$. Dann gibt es verschiedene Punkte p, q und Kreise $\alpha, \beta \neq \alpha$, $\gamma \neq \beta$ durch p, q mit $\varphi = (\alpha\beta;\, p)$, $\psi = (\beta\gamma;\, p)$. Damit ist $\varphi + \psi = (\alpha\gamma;\, p)$ und folglich $\overline{\varphi + \psi} = (\gamma\alpha;\, q)$. Wegen $\bar{\varphi} = (\beta\alpha;\, q)$, $\bar{\psi} = (\gamma\beta;\, q)$ hat man $\bar{\psi} + \bar{\varphi} = (\gamma\alpha;\, q) = \overline{\varphi + \psi}$.

Für das betrachtete Beispiel $\mathfrak{W} \cong \mathfrak{S}_3$ ist also der involutorische Antiautomorphismus $\varphi \to \bar{\varphi}$ gewiß nicht die Identität, da sonst $\mathfrak{W}$ abelsch sein müßte.

Daß der Antiautomorphismus $\varphi \to \bar{\varphi}$ involutorisch ist, kann man sich zur Verpflanzung eines Winkels in irgendeinen vorgegebenen Punkt zunutze machen: Sind paarweise verschiedene Kreise α, β, γ durch den Punkt p gegeben mit $\alpha \cap \beta = \{p, q\}$, $p \neq q$, $\beta \cap \gamma = \{p, r\}$, $p \neq r$, $\gamma \cap \alpha = \{p\}$, so folgt mit $\bar{\bar{\varphi}} = \varphi$, $\varphi = (\alpha\beta;\, q)$ die Aussage

$$(\alpha\beta;\, q) \equiv \overline{\overline{(\alpha\beta;\, q)}} \equiv \overline{(\beta\alpha;\, p)} \equiv \overline{(\beta\gamma;\, p)} \equiv (\gamma\beta;\, r).$$

Literaturverzeichnis.

[1] *E. Artin*, Geometric Algebra. New York, London 1957.

[2] *R. Baer*, Free Mobility and Orthogonality. Trans. Amer. Math. Soc. **68** (1950), 439—460.

[3] *R. Baer*, Linear algebra and projective geometry. New York 1952.

[4] *W. Benz*, Axiomatischer Aufbau der Kreisgeometrie auf Grund von Doppelverhältnissen. J. reine angew. Math. **199** (1958), 56—90.

[5] *W. Benz*, Zur Theorie der Möbiusebenen. I. Math. Ann. **134** (1958), 237—247.

[6] *W. Benz*, Beziehungen zwischen Orthogonalitäts- und Anordnungseigenschaften in Kreisebenen. Math. Ann. **134** (1958), 385—402.

[7] *W. Benz*, $(8_3, 6_4)$-Konfigurationen in Laguerre-, Möbius- und weiteren Geometrien. Math. Z. **70** (1958), 283—296.

[8] *G. Ewald*, Axiomatischer Aufbau der Kreisgeometrie. Math. Ann. **131** (1956), 354—371.

[9] *G. Ewald*, Über eine Berührgenschaft von Kreisen. Math. Ann. **134** (1957), 58—61.

[10] *A. J. Hoffman*, On the foundations of inversion geometry. Trans. Amer. Math. Soc. **71** (1951), 218—242.
[11] *B. de Kérékjarto*, Sur le caractère topologique du groupe homographique de la sphère. Acta Math. **74** (1941), 311—341.
[12] *F. Möbius*, Gesammelte Werke (hier: Theorie der Kreisverwandtschaft). Leipzig 1886.
[13] *B. Petkantschin*, Axiomatischer Aufbau der zweidimensionalen Möbiusschen Geometrie. Annuaire Univ. Sofia II, Fac. Phys.-Math. **1** (1940), 219—325.
[14] *L. J. Smid*, Over Cirkelmeetkunden. Groningen 1928.
[15] *W. Süss*, Beiträge zur gruppentheoretischen Begründung der Geometrie. III. Tohoku Math. J. **28** (1927), 228—241.
[16] *J. Tits*, Généralisations des Groupes Projectifs. Acad. Roy. Belg. Bull. Cl. Sci. **35** (1949), 197—208, 224—233, 569—589, 756—773.
[17] *B. L. v. d. Waerden, L. J. Smid*, Eine Axiomatik der Kreisgeometrie und der Laguerregeometrie. Math. Ann. **110** (1935), 753—776.
[18] *H. Zassenhaus*, Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. Abh. Math. Sem. Hambg. **11** (1936), 17—40.
[19] *H. Zassenhaus*, Über endliche Fastkörper. Abh. Math. Sem. Hambg. **11** (1936), 187—220.

Eingegangen 1. September 1959.

Singularities of Solutions to the Wave Equation in Three Dimensions.

By *R. P. Gilbert* at Pittsburgh (Pennsylvania, U.S.A.).

Résumé.

Die Singularitäten dreidimensionaler, von einem Whittaker-Bergmanschen Operator erzeugter Wellenfunktionen werden an Hand einer Erweiterung eines Begriffs untersucht, der zuerst von Hadamard (im Beweise eines berühmten „Satzes" über die Multiplikation von Singularitäten) eingeführt worden ist; die Erweiterung ist vom Verfasser bereits zum Studium harmonischer Funktionen in drei Dimensionen entwickelt worden. Obwohl von recht allgemeinem Charakter, erweisen sich die erzielten Ergebnisse als oft schwierig anwendbar, weshalb einige einfachere Analogien für bestimmte Typen von Wellenfunktionen ebenfalls entwickelt werden, namentlich axial-symmetrische Funktionen und solche, die mit Stieltjes' Verfahren dargestellt werden.

Abstract.

The singularities of three-dimensional wave functions generated by a Whittaker-Bergman operator are investigated by means of an extension to a concept used originally by Hadamard (in the proof of his celebrated theorem on the multiplication of singularities), which was previously developed by the author for the study of harmonic functions in three dimensions. The results obtained though quite general are often difficult to apply, hence some simpler analogies for special types of wave functions, axially symmetric ones and those developed by Stieltjes' method, are also developed.

I. Introduction.

The four-dimensional Laplace equation

$$\Box \Phi \equiv \sum_{\nu=1}^{4} \frac{\partial^2 \Phi}{\partial x_\nu^2} = 0,$$

becomes the wave equation in three dimensions,

$$\Delta \Phi - \frac{1}{c^2} \frac{\partial^2 \Phi}{\partial t^2} \equiv \sum_{\nu=1}^{3} \frac{\partial^2 \Phi}{\partial x_\nu^2} - \frac{1}{c^2} \frac{\partial^2 \Phi}{\partial t^2} = 0,$$

when the variable x_4 is replaced by ict. Consequently, any investigation of the singularities of solutions to one equation results in a study of singularities of solutions to the other equation, when the arguments are continued to complex values. Solutions to $\Box \Phi = 0$, may be constructed by a modified form of the Whittaker operator [1], [2], [3].

This operator transforms functions of three complex variables $F(\tau, u, v)$, into harmonic functions of four variables[1]).

$$H(X) \equiv B_4\,(F, L_u, L_v, X^0) = \frac{-1}{4\pi^2} \int\limits_{L_u} \int\limits_{L_v} F(\tau, u, v) \frac{dv}{v} \frac{du}{u},$$

where

$$\tau = ix_1\left(1 - \frac{1}{uv}\right) - ix_2\left(\frac{1}{v} + \frac{1}{u}\right) + x_3\left(\frac{1}{v} - \frac{1}{u}\right) + x_4\left(1 + \frac{1}{uv}\right),$$

$$|\,X - X^0\,| < \varepsilon, \;\; X \equiv (x_1, x_2, x_3, x_4), \;\; X^0 \equiv (x_1^0, x_2^0, x_3^0, x_4^0),$$

where L_u and L_v are closed differentiable arcs in the u and v planes respectively, and $\varepsilon > 0$ is sufficiently small.

One may realize how this operator transforms the functions $F(\tau, u, v)$ into the harmonic functions $H(X)$, by first considering the generating function for the homogeneous, harmonic polynomials of degree n, defined by

$$\tau^n \equiv \left[ix_1\left(1 - \frac{1}{uv}\right) - ix_2\left(\frac{1}{u} + \frac{1}{v}\right) + x_3\left(\frac{1}{v} - \frac{1}{u}\right) + x_4\left(1 + \frac{1}{uv}\right)\right]^n$$

$$= \sum_{k,l=0}^{n} H_n^{k,\,l}\,(X)\, u^{-k}\, v^{-l}.$$

The $H_n^{k,\,l}\,(X)$ are linearly independent polynomials, which form a complete system [4]. Consequently any harmonic function $H(X)$ regular about $X = 0$, may be expanded in terms of these polynomials. Furthermore, from their generating function, it follows that

$$H_n^{k,\,l}\,(X) = \frac{-1}{4\pi^2} \int\limits_{L_u} \int\limits_{L_v} \tau^n\, u^k\, v^l \frac{dv}{v} \frac{du}{u},$$

where the paths of integration are taken to be unit circles.

A reciprocal Whittaker operator may be obtained, such that given a harmonic function $H(X)$, one may construct a function $F(\tau, u, v)$. In contrast to the three-dimensional case the function $F(\tau, u, v)$ will not be identical with the one which generated $H(X)$ [5]. To do this we introduce the surface harmonics

$$S_n^{k,\,l}\,(\theta_1, \theta_2, \varphi) = \frac{H_n^{k,l}(X)}{\varrho^n \binom{n}{k}},$$

where

$$\begin{aligned} x_1 &= \varrho \cos\theta_1, \\ x_2 &= \varrho \sin\theta_1 \cos\theta_2, \\ x_3 &= \varrho \sin\theta_1 \sin\theta_2 \cos\varphi, \\ x_4 &= \varrho \sin\theta_1 \sin\theta_2 \sin\varphi, \end{aligned}$$

and

$$\varrho \geqq 0, \;\; 0 \leqq \theta j \leqq \pi \;\; (j = 1, 2), \;\; 0 \leqq \varphi \leqq 2\pi,$$

which form a complete set of orthogonal functions on the unit hypersphere. Using the generating function rewritten in hyperspherical coordinates as

$$\tau^n = \sum_{k,l} \binom{n}{k} \varrho^n S_n^{k,\,l}\,(\theta_1, \theta_2, \varphi)\, u^{-k} v^{-l}$$

---

[1]) This notation has been adapted after S. Bergman; see references [2] and [3].

we construct the kernel

$$K = \frac{1}{(1-\sigma\tau)^2}$$
$$= \sum_{n=0}^{\infty} (n+1)(\sigma\tau)^n$$
$$= \sum_{n=0}^{\infty} \sum_{k,l=0}^{n} (n+1) \binom{n}{k} (\sigma\varrho)^n S_n^{k,l}(\theta_1, \theta_2, \varphi)\, u^{-k} v^{-l}.$$

Now, because of the orthogonality relations over the hypersphere

$$\int_\Omega S_n^{k,l} \overline{S_n^{k',l'}}\, d\Omega = \delta_{kk'} \delta_{ll'} \frac{\binom{n}{l}}{\binom{n}{k}},$$

(where $d\Omega = \sin^2\theta_1 \sin\theta_2 d\theta_1 d\theta_2 d\varphi$) we see that

$$\frac{1}{2\pi^2} \int_\Omega (1-\sigma\tau)^{-2} \overline{S_n^{k,l}} d\Omega = \binom{n}{l} \sigma^n u^{-k} v^{-l}.$$

Consequently, given a harmonic function

$$H(X) \equiv V(\varrho, \theta_1, \theta_2, \varphi) = \sum_{n=0}^{\infty} \sum_{k,l=0}^{n} a_{nkl} \binom{n}{k} \varrho^n S_n^{k,l}(\theta_1, \theta_2, \varphi),$$

one may generate the function

$$F(\sigma, u, v) = \sum_{n=0}^{\infty} \sum_{k,l=0}^{n} a_{nkl} \binom{n}{l} \sigma^n u^{-k} v^{-l}$$

by the integral operator

$$F(\sigma, u, v) = \frac{1}{2\pi^2} \int_\Omega \frac{\overline{V(\varrho, \theta_1, \theta_2, \varphi)}}{(1-\sigma\tau)^2} d\Omega.$$

II. Singularities of Four-Dimensional Harmonic Functions.

In a previous paper, the author proved the following theorem:

Theorem 1. *If $z^3 \equiv E\,\{S(x_1, x_2, x_3, u) = 0\}$ is the singularity manifold of $\frac{1}{u} f(t, u)$, then*

$$H(x_1, x_2, x_3) = \frac{1}{2\pi i} \int_L f(t, u) \frac{du}{u}$$

(where L is the unit circle) is regular at (x_1, x_2, x_3) providing this point does not lie simultaneously on the two surfaces

$$S(x_1, x_2, x_3, u) = 0,$$

and

$$\frac{\partial}{\partial u} S(x_1, x_2, x_3, u) = 0.$$

In this section a similar result will be obtained in the case of four-dimensional harmonic functions.

Theorem 2. *Let $Z^4 \equiv E\{S(X, u, v) = 0\}$ be the singularity manifold of $\frac{1}{uv} F(\tau, u, v)$, then*

$$H(X) = -\frac{1}{4\pi^2} \int_{L_u} \int_{L_v} F(\tau, u, v) \frac{dv}{v} \frac{du}{u}$$

is regular at $X \in C^4$ (where C^4 is a region in the ideal, Euclidean four-space, that is the four-dimensional space of complex points), providing $X \notin$ on the "envelope" of $S(X, u, v) = 0$.

Proof. The proof of this theorem closely parallels the one for Theorem 1. As before we consider the analytic continuation of $H(X)$ along a curve $\Gamma(X) \in C^4$ starting at the origin $(0, 0, 0, 0)$.

The integral representation of

$$H(X) = \frac{-1}{4\pi^2} \int_{L'_u} \int_{L'_v} F(\tau, v, u) \frac{dv}{v} \frac{du}{u}$$

(where L'_u and L'_v are taken to be unit circles) will remain the same if either integration path is continuously deformed in such a manner so that at no time they cross a singularity of $\frac{1}{uv} F(\tau, u, v)$. Therefore, we may write $H(X)$ as

$$H(X) = -\frac{1}{4\pi^2} \int_{L_u} \int_{L_v} F(\tau, u, v) \frac{dv}{v} \frac{du}{u}$$

where L_u and L_v are new integration paths obtained by observing the above precautions.

Since τ is dependent on X, the singularities of the integrand move in the u and v planes as $H(X)$ is continued along $\Gamma(X)$. Now, as long as we can avoid crossing such a singularity by deforming either L_u or L_v, we may still be able to continue $H(X)$ further. For instance, in order to avoid crossing an advancing singularity in the u-plane, we may suitably deform the contour L_u. However, we must be sure that in doing this no singularity in the v-plane crosses L_v.

Let us assume that we have been able to continue $H(X)$ to the point X', and let us consider the singularities of the integrand for $X = X'$; these singularities may be represented implicitly by

$$S(X', u, v) = 0.$$

Let us suppose there is a singularity at $u = \alpha$, and one at $v = \beta$, which L_u and L_v respectively are in danger of crossing. By expanding $S(X', u, v)$ in a double Taylor series about (α, β) one obtains

$$S(X', u, v) = (u - \alpha) \frac{\partial S}{\partial u} + (v - \beta) \frac{\partial S}{\partial v}$$
$$+ \frac{1}{2} \left[(u - \alpha)^2 \frac{\partial^2 S}{\partial u^2} + 2(u - \alpha)(v - \beta) \frac{\partial^2 S}{\partial u \partial v} + (v - \beta)^2 \frac{\partial^2 S}{\partial v^2} \right] + \cdots.$$

Now, unless the first variation of $S(X', u, v)$ vanishes at (α, β), $S(X, u, v)$ may be approximated as

$$S(X', u, v) \cong (u - \alpha) \frac{\partial S}{\partial u} + (v - \beta) \frac{\partial S}{\partial v}$$

in a bicylindrical neighborhood of (α, β),

$$|u - \alpha| < \varepsilon_1, \quad |v - \beta| < \varepsilon_2.$$

In this case it is always possible to choose a secant to the circle $|u-\alpha| = \frac{\varepsilon_1}{2}$ not passing through $u = \alpha$, and a secant to the circle $|v-\beta| = \frac{\varepsilon_2}{2}$ not passing through $v = \beta$, such that $S(X, u, v) \neq 0$ on those portions of the secants inside the respective circles. It follows in this case, that we may deform the paths L_u and L_v so that they follow the secants about the singular point (α, β) and thereby continue $H(X)$ still further. The only possible singularities of $H(X)$ are therefore, those values of X satisfying simultaneously

$$S(X, u, v) = 0,$$

and

$$\frac{\partial S}{\partial u} + \frac{\partial S}{\partial v}\pi'(u) = 0,$$

where $v = \pi(u)$ is an arbitrary relationship between u and v. This completes our proof.

Using the language of real geometry we may say that unless we are in the neighborhood of the envelope $\varepsilon(X) = 0$ to $S(X, u, v) = 0$ [in which case there are an infinite number of such surfaces tangent to $\varepsilon(X) = 0$] we may avoid crossing these singularities by deforming L_u or L_v.

III. Singularities of Certains Types of Wave Functions.

If in Theorem 2, the coordinate x_4 is replaced by ict, the corresponding result for wave functions is obtained. This result, though quite general, is often difficult to apply. Hence, in this section some simpler analogies for certain special types of wave functions will be discussed.

A. Singularities of Stieltjes' Solutions.

If x_1, x_2, x_3, and $x_4 = ict$, are replaced by the following,

$$\begin{aligned} x_1 &= s\cos\theta\cos\varphi, \\ x_2 &= s\cos\theta\sin\varphi, \\ x_3 &= s\sin\theta\cos\chi, \\ ict &= s\sin\theta\sin\chi \end{aligned}$$

the wave equation may be written in the form

$$\frac{\partial^2\Phi}{\partial s^2} + \frac{3}{s}\frac{\partial\Phi}{\partial s} + \frac{1}{s^2}\frac{\partial^2\Phi}{\partial\Theta^2} + \frac{1}{s^2\cos_\mu{}^2\Theta}\frac{\partial^2\Phi}{\partial\varphi^2} + \frac{1}{s^2\sin^2\Theta}\frac{\partial^2\Phi}{\partial x^2} + \frac{\cot\Theta - \operatorname{ton}\Theta}{s^2}\frac{\delta\Phi}{\delta\Theta} = 0.$$

Setting $\mu = \cos(2\theta)$, elementary solutions of degree $2n$ may be found having the form [6]

$$\Phi = s^{2n}\Theta(\mu)\, e^{im\varphi + ip\chi},$$

where $\Theta(\mu)$ satisfies

$$\frac{d}{d\mu}\left\{(1-\mu^2)\frac{d\Theta}{d\mu}\right\} + \Theta\left\{n(n+1) - \frac{m^2}{2(1+\mu)} - \frac{p^2}{2(1-\mu)}\right\} = 0.$$

$\Theta(\mu)$ then is the hypergeometric function

$$(1+\mu)^{\frac{m}{2}}(1-\mu)^{\frac{p}{2}} F\left(n+1+\frac{m+p}{2}, \frac{m+p}{2} - n, p+1; \frac{1-\mu}{2}\right),$$

which becomes the associated Legendre function $P_n^m(\cos 2\theta)$ when $m = p$ [6]. We realize therefore, if $V(r, \theta, \varphi)$ is a harmonic function $V(s^2, 2\theta, \Phi + \chi)$ is a wave function. The harmonic functions regular at the origin are obtained from the Whittaker-Bergman operator [2], [3]. In spherical coordinates this operator may be written as [5]

$$V(r, \theta, \varphi) \equiv B_3(f, L, P_0) = \frac{1}{2\pi i}\int_L f(\tau, u)\,\frac{du}{u},$$

$$\tau = r\left\{\cos\theta + \frac{i}{2}\sin\theta\left[\frac{u}{e^{i\varphi}} + \frac{e^{i\varphi}}{u}\right]\right\},$$

$$|P - P_0| < \varepsilon,\ P \equiv (r, \theta, \varphi),\ P_0 \equiv (r_0, \theta_0, \varphi_0),$$

where L is a closed differentiable arc in the u-plane, and $\varepsilon > 0$ is sufficiently small[2]). Hence, we state without proof the following result which is an immediate extension of Theorem 1.

Theorem 3. *Let*

$$\Phi(s, \theta, \varphi, \chi) \equiv V(s^2, 2\theta, \varphi + \chi)$$

(where $s^2 = x_1^2 + x_2^2 + x_3^2 - c^2t^2$) be a wave function obtained from a Whittaker-type operator, that is

$$V(s^2, 2\theta, \varphi + \chi) = \frac{1}{2\pi i}\int_L f(\tau, u)\,\frac{du}{u},$$

$$\tau = s^2\left\{\cos 2\theta + \frac{i}{2}\sin 2\theta\left[\frac{u}{e^{i(\varphi+\chi)}} + \frac{e^{i(\varphi+\chi)}}{u}\right]\right\},$$

and L is the unit circle, etc. Furthermore, let

$$Z^4 \equiv E\{G(s, \theta, \varphi, \chi \mid u) = 0\}$$

be the singularity manifold of $\frac{1}{u} f(\tau, u)$, then $\Phi(s, \theta, \Phi, \chi)$ is regular at (s, θ, Φ, χ) providing this "point" does not lie simultaneously on the two surfaces

$$G(s, \theta, \Phi, \chi \mid u) = 0,$$

and

$$g(s, \theta, \Phi, \chi \mid u) = 0.$$

Having reduced the problem in this case to the study of harmonic functions many interesting results are immediately obtainable from the existing literature.

B. Singularities of Axially Symmetric Wave Functions.

In cylindrical coordinates the wave equation becomes

$$\frac{\partial^2\Phi}{\partial\varrho^2} + \frac{1}{\varrho}\frac{\partial\Phi}{\partial\varrho} + \frac{1}{\varrho^2}\frac{\partial^2\Phi}{\partial\varphi^2} + \frac{\partial^2\Phi}{\partial x_3^2} - \frac{1}{c^2}\frac{\partial^2\Phi}{\partial t^2} = 0.$$

A particular solution of this equation which represents a wave function symmetric above the x_3 axis is [6]

$$\Phi(\varrho, \varphi, x_3, t) = \frac{1}{2\pi i}\int_L F(\sigma, \tau)\,\frac{du}{u},$$

---

[2]) From Heine's integral representation for the associated Lengendre functions [7]

$$\frac{1}{2\pi i}\int_L \tau^n u^m\,\frac{du}{u} = \frac{n!}{(n+m)!}\,r^n P_n^m(\cos\theta)\,e^{im\varphi}$$

(where L is say the unit circle) it follows that if $V(r, \theta, \Phi)$ is regular at the origin it may be generated from a function of two complex variables of the form $f(\tau, u) = \sum_{n=0}^{\infty}\sum_{m=-n}^{+n} a_{nm}\,\tau^n u^m$.

where

$$\sigma = z + \frac{i\varrho}{2}\left(u + \frac{1}{u}\right), \quad \tau = t + \frac{i\varrho}{2}\left(u - \frac{1}{u}\right),$$

and L is the unit circle. The general locus for the singularities of the integral may be expressed as

$$\Psi(\sigma, \tau) \equiv G(\varrho, \varphi, x_3, t \mid u) = 0.$$

Hence, we may again extend our result of Theorem 1 to include this case.

Theorem 4. *Let*

$$Z^4 \equiv E\{G(\varrho, \varphi, x_3, t \mid u) = 0\}$$

be the singularity manifold of $\frac{1}{u} F(\sigma, \tau)$, *then*

$$\Phi(\varrho, \varphi, x_3, t) = \frac{1}{2\pi i} \int_L F(\sigma, \tau) \frac{du}{u}$$

is regular at $(\varrho, \varphi, x_3, t)$ *providing this "point" does not lie simultaneously on the two surfaces*

$$G(\varrho, \varphi, x_3, t \mid u) \equiv \Psi(\sigma, \tau) = 0,$$

and

$$\frac{\partial G}{\partial u} \equiv \frac{\partial \psi}{\partial \sigma} \frac{\partial \sigma}{\partial u} + \frac{\partial \psi}{\partial \tau} \frac{\partial \tau}{\partial u} = 0.$$

References.

[1] *E. T. Whittaker* and *G. N. Watson*, A course of modern analysis, 1920.

[2] *S. Bergman*, Zur Theorie der algebraischen Potentialfunktionen des dreidimensionalen Raumes, Math. Ann. **99** (1928), 629—659.

[3] *S. Bergman*, Essential singularities of solutions of a class of linear partial differential equations in three variables, J. Rational Mech. and Anal. **3** (1954), 539—560.

[4] *A. Erdelyi*, Higher transcendental functions, 1953.

[5] *R. Gilbert*, Singularities of three dimensional harmonic functions, doctoral dissertation, Carnegie Institute of Technology, 1958 (to be published in the Pacific Journal of Mathematics).

[6] *H. Bateman*, Electrical and optical wave-motion, 1914.

[7] *P. M. Morse* and *H. Feshbach*, Methods of theoretical physics II, 1953.

Eingegangen 25. September 1959.

Einige Abschätzungen für Abschnittsbasen.

Von *Erich Härtter* in Mainz.

Die vorliegende Arbeit zerfällt in zwei Teile. Im ersten Teil werden Abschnittsbasen für endliche Abschnitte der Menge der nichtnegativen ganzen Zahlen betrachtet, währenddem der zweite Teil eine Verallgemeinerung dieser Fragestellung auf endliche Mengen von Gitterpunkten (Vektoren) von zwei und mehr Dimensionen enthält. Dabei ist der zweite Teil, was die Beweisführung anlangt, vom ersten unabhängig.

I.

1. *Definitionen.* Die (endliche) Menge der nichtnegativen ganzen Zahlen $\{0, 1, 2, \ldots, n\}$ bezeichnen wir abkürzend mit $[0, n]$.

Definition 1. *Seien n und h natürliche Zahlen. Unter einer* Abschnittsbasis *der Ordnung h für n verstehen wir eine Menge $\mathfrak{A} \leqq [0, n]$ mit der Eigenschaft*

$$h\mathfrak{A} \geqq [0, n],$$

d. h. jede Zahl $z \in [0, n]$ ist als Summe von h Summanden aus $\mathfrak{A}$ darstellbar. — Die Anzahl der von 0 verschiedenen Elemente in $\mathfrak{A}$ bezeichnen wir mit $A(n)$.

Definition 2. *Seien h und k gegebene natürliche Zahlen. Sei $n_h(k)$ die größte natürliche Zahl, so daß es eine Abschnittsbasis $\mathfrak{A}$ der Ordnung h für $n_h(k)$ mit*

$$A\left(n_h(k)\right) = k$$

gibt. Eine solche Abschnittsbasis nennen wir eine zu $n_h(k)$ gehörige extremale Abschnittsbasis (Rohrbach [1], Stöhr [2]).

2. Die Folge der Zahlen $n_h(k)$ bildet für festes h und $k = 1, 2, \ldots$ eine monotone zahlentheoretische Funktion. Offenbar ist $n_h(1) = h$ und $n_1(k) = k$. Ferner zeigte Stöhr [2]

$$n_h(2) = \left[\frac{h^2 + 6h + 1}{4}\right]. \tag{1}$$

Im übrigen sind für $n_h(k)$ Abschätzungen bekannt. Wir wollen hier nur Abschätzungen nach unten betrachten. Man gewinnt diese durch Konstruktion geeigneter Abschnittsbasen der Ordnung h, die k positive Elemente enthalten. So bewies Rohrbach [1]

$$n_h(k) > \left(\frac{k}{h}\right)^h \quad \text{für } k > h \geqq 3 \tag{2}$$

und im Spezialfall $h = 2$ für $k \geqq 12$ und $k \equiv 0 \pmod 2$

$$n_2(k) \geqq \frac{k^2}{4} + 2k - \gamma, \tag{3}$$

wobei $\gamma = 6$ bzw. 7 ist, je nachdem $k \equiv 0$ oder $2 \pmod 4$ ist, und für $k \geqq 43$ und $k \equiv 1 \pmod 2$

$$n_2(k) \geqq \frac{k^2}{4} + \frac{11}{6}k - \gamma', \tag{4}$$

wobei $\gamma' = \frac{217}{12}, \frac{237}{12}, \frac{185}{12}, \frac{157}{12}, \frac{153}{12}, \frac{173}{12}$ bezüglich zu setzen ist für $k \equiv 1, 3, 5, 7, 9, 11 \pmod{12}$.

Wir wollen hier eine Rekursionsformel herleiten, die es gestattet, aus einer Abschätzung für die Funktionswerte von $n_{h-1}(k)$ eine Abschätzung für $n_h(k)$ zu finden.

3. Rekursionsformel. Sei schon gezeigt, daß es eine Abschnittsbasis $\mathfrak{A}_{h-1}$ der Ordnung $h-1$ mit u positiven Elementen für die Zahl

$$N_{h-1} \geqq \varphi_{h-1}(u) \quad (h > 2,\ u \geqq u_{h-1} > 0)$$

mit einer positiven Funktion $\varphi_{h-1}(u)$ gibt[1]). Dann bildet

$$\begin{aligned}\mathfrak{A}_h &= \mathfrak{A}_{h-} \cup \{N_{h-1}+1,\ 2N_{h-1}+4,\ 3N_{h-1}+7,\ 4N_{h-1}+10, \ldots, s(N_{h-1}+3)-2\}\\ &= \mathfrak{A}_{h-1} \cup \{x \equiv -2 \pmod{N_{h-1}+3};\ \ x \leqq s(N_{h-1}+3)-2\}^{2})\end{aligned}$$

eine Abschnittsbasis der Ordnung h mit $u + s = k$ positiven Elementen für die Zahl $N_h = s(N_{h-1}+3) - 2 + N_{h-1} + 2 = (s+1)(N_{h-1}+3) - 3$.

Die Basiseigenschaft von $\mathfrak{A}_h$ erkennt man sofort aus der Tatsache, daß alle Zahlen $z \in [0, N_{h-1}+2]$ nach Voraussetzung, bzw. weil 1 und $N_{h-1}+1$ in $\mathfrak{A}_h$ liegen, als Summe von höchstens $h-1$ Summanden aus $\mathfrak{A}_h$ darstellbar sind. Eine Zahl z mit $\alpha(N_{h-1}+3) - 2 \leqq z < (\alpha+1)(N_{h-1}+3) - 2$ $(1 \leqq \alpha \leqq s)$ hat also eine Darstellung

$$z = \big(\alpha(N_{h-1}+3) - 2\big) + \sum_{\nu=1}^{h-1} a_\nu \quad (a_\nu \in \mathfrak{A}_h).$$

Ist nun k vorgegeben, so wollen wir u (und damit auch s) so wählen, daß N_h möglichst groß wird. Wir wählen dazu

$$u = \left[\frac{(k+1)(h-1)}{h}\right] \qquad \left(k \geqq \max\left(h, \frac{hu_{h-1}}{h-1}\right)\right).$$

Wegen $k \geqq h$ gilt dann $u \leqq \frac{(k+1)(h-1)}{h} < k$. Somit folgt mit $s = k - u$

$$\begin{aligned}N_h &\geqq \left(k - \frac{(k+1)(h-1)}{h} + 1\right)\left(\varphi_{h-1}\left(\left[\frac{(k+1)(h-1)}{h}\right]\right) + 3\right) - 3\\ &\geqq \frac{k+1}{h}\left(\varphi_{h-1}\left(\left[\frac{(k+1)(h-1)}{h}\right]\right) + 3\right) - 3 \text{ für } k \geqq \max\left(h, \frac{hu_{h-1}}{h-1}\right).\end{aligned}$$

Setzen wir in obiger Konstruktionsmethode $\varphi_{h-1}(u) = n_{h-1}(u)$, so folgt, weil $n_h(k) \geqq N_h$ ist, als Abschätzung für $n_h(k)$

$$n_h(k) \geqq \max_{1 \leqq u \leqq k} \{(k - u + 1)\big(n_{h-1}(u) + 3\big) - 3\}$$

und mit $u = \left[\frac{(k+1)(h-1)}{h}\right]$

$$n_h(k) \geqq \frac{k+1}{h}\left(n_{h-1}\left(\left[\frac{(k+1)(h-1)}{h}\right]\right) + 3\right) - 3 \quad (k \geqq h).$$

---

[1]) Hierbei hängt natürlich auch N_{h-1} von u ab.

[2]) Das Symbol $\{x \equiv a \pmod m;\ x \leqq k\}$ bedeutet die Menge der nichtnegativen ganzen Zahlen aus der angegebenen Restklasse unterhalb der betreffenden Schranke.

Der wichtigste Fall ist, daß wir für $\varphi_{h-1}(u)$ ein Polynom $(h-1)$-ten Grades

$$\varphi_{h-1}(u) = \frac{u^{h-1}}{(h-1)^{h-1}} + c_{h-1}u^{h-2} \quad (h > 2,\ u \geqq u_{h-1} > 0,\ c_{h-1} > 0)$$

setzen. Dann erhalten wir wegen $u \geqq \frac{(k+1)(h-1)}{h} - \frac{h-1}{h} = \frac{k(h-1)}{h}$

$$N_h \geqq \frac{k+1}{h}\left(\frac{k^{h-1}}{h^{h-1}} + c_{h-1}\frac{k^{h-2}(h-1)^{h-2}}{h^{h-2}} + 3\right) - 3,$$

also

$$(5) \qquad n_h(k) \geqq N_h \geqq \frac{k^h}{h^h} + \frac{k^{h-1}}{h^h} + c_{h-1}\frac{(h-1)^{h-2}}{h^{h-1}}k^{h-1} + c_{h-1}\frac{(h-1)^{h-2}}{h^{h-1}}k^{h-2}$$
$$+ 3\frac{k+1}{h} - 3 \quad \text{für } k \geqq \max\left(h, \frac{hu_{h-1}}{h-1}\right).$$

Diese Abschätzung (5) stellt eine Verbesserung der Abschätzung (2) dar.

4. Um eine Abschätzung für $n_3(k)$ zu erhalten, benutzen wir (3) und (4). Zunächst betrachten wir $u = \left[\frac{(k+1)2}{3}\right] \equiv 0 \pmod 2$, d. h. $k \equiv 0, 2 \pmod 3$, und setzen

$$N_2 = \varphi_2(u) = \frac{u^2}{4} + 2u - \gamma \quad (u \geqq u_2 \geqq 12).$$

Damit ergibt sich

$$n_3(k) \geqq \frac{k^3}{27} + \frac{13}{27}k^2 + \frac{13}{9}k - \gamma\frac{k+1}{3} - 2 \quad \text{für } k \geqq \frac{3u_2}{2}.$$

Im Fall $u = \left[\frac{(k+1)2}{3}\right] \equiv 1 \pmod 2$, d. h. $k \equiv 1 \pmod 3$, folgt

$$N_2 = \varphi_2(u) = \frac{u^2}{4} + \frac{11}{6}u - \gamma' \quad (u \geqq u_2 \geqq 43)$$

und

$$n_3(k) \geqq \frac{k^3}{27} + \frac{12}{27}k^2 + \frac{38}{27}k - \gamma'\frac{k+1}{3} - 2 \quad \text{für } k \geqq \frac{3u_2}{2}.$$

In dieser Weise fortfahrend lassen sich nun auch für höhere Ordnungen Abschätzungen für $n_h(k)$ berechnen. Berücksichtigt man in (5) nur Glieder der h-ten und $(h-1)$-ten Potenz von k und setzt man den Koeffizienten von k^{h-1}

$$\frac{1 + c_{h-1}h(h-1)^{h-2}}{h^h} = c_h,$$

so läßt sich durch Induktion für $h \geqq 4$ leicht beweisen

$$c_h > \frac{1 + c_2 2h}{h^h} > \frac{2c_2}{h^{h-1}}$$

mit $c_2 = 2$ bzw. $\frac{11}{6}$, je nachdem $k \equiv 0, 2$ bzw. $1 \pmod 3$ ist. Also haben wir

$$n_h(k) > \frac{k^h}{h^h} + \frac{2c_2}{h^{h-1}}k^{h-1}.$$

5. Für $n_3(k)$ erhält man auf folgende Art noch eine etwas bessere Abschätzung: Die Zahlenmenge $\mathfrak{A}_2 = \{0, 1, 2, \ldots, t+1, 2t+3, 3t+5, \ldots st+2s-1\}$ ist — wie man sofort erkennt — Basis 2-ter Ordnung für $N_2 = st + 2s - 1 + t + 1 = (s+1)(t+1) + s - 1$ mit $t + s = u$ positiven Elementen. Für ungerades u und $t = \frac{u-1}{2}$ erhält man

$N_2 = \frac{u^2 + 6u + 1}{4}$ und für gerades u und $t = \frac{u-2}{2}$ oder $t = \frac{u}{2}$ folgt $N_2 = \frac{u^2 + 6u}{4}$. Insgesamt können wir also schreiben

$$N_2 = \left[\frac{u^2 + 6u + 1}{4}\right]. \tag{6}$$

Hieraus konstruieren wir eine Basis 3-ter Ordnung für

$$\begin{aligned} N_3 &= sN_2 + s + \left[\frac{u+1}{2}\right](s-1) + s - 1 + N_2 + 1 + \left[\frac{u+1}{2}\right] \\ &= (s+1)(N_2+1) + \left[\frac{u+1}{2} + 1\right] s - 1 \end{aligned}$$

durch

$$\begin{aligned} \mathfrak{A}_3 = \mathfrak{A}_2 \cup \Big\{ & N_2 + 1, 2N_2 + 2 + \left[\frac{u+1}{2}\right] + 1, 3N_2 + 3 + 2\left[\frac{u+1}{2}\right] + 2, \ldots, \\ & sN_2 + s + \left[\frac{u+1}{2}\right](s-1) + s - 1 \Big\}. \end{aligned}$$

Die Basiseigenschaft folgt aus der Tatsache, daß alle Zahlen $z \in \left[0, N_2 + 1 + \left[\frac{u+1}{2}\right]\right]$ als Summe von zwei Summanden aus $\mathfrak{A}_3$ darstellbar sind, denn $\left[0, \left[\frac{u+1}{2}\right]\right] < \mathfrak{A}_2$. Die Menge $\mathfrak{A}_3$ enthält $u + s = k$ positive Elemente und N_2 hängt nach (6) von u ab. Wir wählen $u = \left[\frac{2k-2}{3}\right]$ und erhalten für $n_3(k)$ die Abschätzung

$$\begin{aligned} n_3(k) \geqq N_3 &\geqq \left(k - \frac{2k-2}{3} + 1\right)\left(\frac{\left(\frac{2k-2}{3} - \frac{2}{3}\right)^2 + 6\left(\frac{2k-2}{3} - \frac{2}{3}\right) + 2}{4}\right) \\ &\quad + \left(\frac{\frac{2k-2}{3} - \frac{2}{3} + 2}{2}\right)\left(k - \frac{2k-2}{3}\right) - 1 \\ &\geqq \frac{k^3}{27} + \frac{13}{27}k^2 + \frac{49}{54}k - \frac{137}{54}. \end{aligned}$$

Bemerkung. Der Vergleich von (1) und (6) liefert noch

$$n_h(2) \leqq n_2(h),$$

jedoch gilt nicht allgemein $n_3(h) \geqq n_h(3)$, wie Beispiele bei Stöhr [2] zeigen.

6. *Einige weitere Abschätzungen für $n_h(k)$.* Wir nehmen an, daß die Elemente $a_\varkappa$ ($\varkappa = 0, 1, 2, \ldots, k$) einer zu $n_h(k)$ gehörenden Abschnittsbasis $\mathfrak{A}$ der Größe nach geordnet sind, $a_0 = 0$.

Wir wollen beweisen

$$n_h(k + k^* + 1) \geqq n_h(k) + n_h(k^*) - h + 2. \tag{7}$$

Beweis. Sei $\mathfrak{A}$ eine zu $n_h(k)$ gehörende extremale Abschnittsbasis,

$$\mathfrak{A}^* = \{a_0^*, a_1^*, \ldots, a_{n_h(k^*)}^*\}$$

eine zu $n_h(k^*)$ gehörende extremale Abschnittsbasis. Dann ist

$$\mathfrak{A} \cup \left\{\left[\frac{n_h(k)+1}{h}\right] + a_0^*, \left[\frac{n_h(k)+1}{h}\right] + a_1^*, \ldots, \left[\frac{n_h(k)+1}{h}\right] + a_{n_h(k^*)}^*\right\}$$

Abschnittsbasis der Ordnung h für $n_h(k) + n_h(k^*) - h + 2$, weil alle z mit

$$n_h(k) + 1 \leqq z \leqq n_h(k) + n_h(k^*) - h + 2$$

in der Form

$$z = \sum_{\varkappa=1}^{h} \left(\left[\frac{n_h(k) + 1}{h} \right] + a^{*(\varkappa)} \right) = \sum_{\varkappa=1}^{h} \left(\frac{n_h(k) + 1}{h} - \varrho + a^{*(\varkappa)} \right)$$

$$\left(0 \leqq \varrho \leqq \frac{h-1}{h},\ a^{*(\varkappa)} \in \mathfrak{A}^* \right)$$

darstellbar sind.

Hält man in $n_h(k)$ das Argument k fest und läßt h die Werte $1, 2, \ldots$ durchlaufen, so erhält man ebenfalls eine monotone Funktion. Wir zeigen

$$n_{h+1}(k) \geqq n_h(k) \left(1 + \frac{1}{h} \right) \tag{8}$$

und

$$n_{h+1}(k+1) \geqq 2 n_h(k) + 1. \tag{9}$$

Beweis von (8). Sei $\mathfrak{A}$ extremale Abschnittsbasis für $n_h(k)$ und a_k das größte Element in $\mathfrak{A}$. Dann sind alle Zahlen z mit $n_h(k) + 1 \leqq z \leqq n_h(k) + a_k$ darstellbar als

$$z = a_k + \sum_{\varkappa=1}^{h} a^{(\varkappa)} \quad (a^{(\varkappa)} \in \mathfrak{A}).$$

Da $a_k \geqq \frac{n(k)}{h}$ ist, folgt (8).

Beweis von (9). Ist $\mathfrak{A}$ extremale Abschnittsbasis für $n_h(k)$, dann bilden wir

$$\tilde{\mathfrak{A}} = \mathfrak{A} \cup \{n_h(k) + 1\}.$$

$\tilde{\mathfrak{A}}$ ist Abschnittsbasis der Ordnung $h + 1$ für $2 n_h(k) + 1$, womit (9) bewiesen ist.

Zum Schluß zeigen wir noch

$$n_2(k+1) \leqq n_2(k) + n_2(k-1) + 2 \qquad (k \geqq 2). \tag{10}$$

Beweis. Sei $\mathfrak{A} = \{a_0, a_1, \ldots, a_k, a_{k+1}\}$ ($a_\varkappa < a_{\varkappa+1}$ für $\varkappa = 0, 1, 2, \ldots, k$) eine extremale Abschnittsbasis für $n_2(k+1)$. Dann muß $a_\varkappa \leqq n_2(\varkappa - 1) + 1$ ($\varkappa = 2, \ldots, k+1$) gelten, insbesondere also $a_{k+1} \leqq n_2(k) + 1$ und $a_k \leqq n_2(k-1) + 1$. Nun ist für $a_k + 1 < a_{k+1}$, d. h. zwischen a_k und a_{k+1} liegt noch eine natürliche Zahl, $z = a_{k+1} + a_k + 1 \notin 2\mathfrak{A}$, also muß

$$n_2(k+1) \leqq a_{k+1} + a_k \leqq n_2(k) + n_2(k-1) + 2$$

gelten. Für den Fall $a_{k+1} = a_k + 1$ haben wir

$$n_2(k+1) \leqq 2 a_{k+1} = 2 a_k + 2 \leqq 2 n_2(k-1) + 4 \leqq n_2(k) + n_2(k-1) + 2,$$

weil $n_2(k-1) + 2 \leqq n_2(k)$ ist.

II.

7. Wir wollen nun die Ergebnisse, die wir im ersten Teil dieser Arbeit erhalten haben, auf Mengen von Gitterpunkten (Vektoren) übertragen. Dazu treffen wir folgende Bezeichnungen und Definitionen (siehe auch [3]): Wir betrachten Mengen von Vektoren $\mathfrak{z} = \{z_1, \ldots, z_r\}$ im r-dimensionalen Raum ($r \geqq 1$) mit ganzzahligen nichtnegativen Komponenten. Den Nullvektor bezeichnen wir mit $\mathfrak{o}$ und den Vektor $\{n, \ldots, n\}$ mit $\mathfrak{n}$; die Gesamtheit der Vektoren $\mathfrak{z} = \{z_1, \ldots, z_r\}$ mit $0 \leqq z_\varrho \leqq n$ ($\varrho = 1, \ldots, r$) kürzen wir

durch $\mathfrak{Q}_r(\mathfrak{n})$ oder $\mathfrak{Q}_r(n, \ldots, n)$ ab[3]). Die Definition der Summe von Vektoren und von Mengen von Vektoren treffen wir in der üblichen Weise. In Analogie zu Definition 1 und 2 erklären wir nun:

Definition 3. *Seien n, h und r natürliche Zahlen. Unter einer* Abschnittsbasis *der Ordnung h für $\mathfrak{Q}_r(\mathfrak{n})$ ($\mathfrak{n} = \{n, \ldots, n\}$) verstehen wir eine Menge $\mathfrak{A} \leqq \mathfrak{Q}_r(\mathfrak{n})$ mit der Eigenschaft*

$$h\mathfrak{A} \geqq \mathfrak{Q}_r(\mathfrak{n}),$$

d. h. jedes $\mathfrak{z} \in \mathfrak{Q}_r(\mathfrak{n})$ ist als Summe von h Summanden aus $\mathfrak{A}$ darstellbar[4]). Die Anzahl der von $\mathfrak{o}$ verschiedenen Elemente in $\mathfrak{A}$ bezeichnen wir mit $A(\mathfrak{n})$ oder $A(n, \ldots, n)$.

Definition 4. *Seien h, k und r gegebene natürliche Zahlen. Dann sei $n_{h,r}(k)$ die größte ganze Zahl, so daß es eine Abschnittsbasis $\mathfrak{A}$ der Ordnung h für $\mathfrak{Q}_r(\mathfrak{n}_{h,r}(k))$ mit*

$$A(\mathfrak{n}_{h,r}(k)) = k$$

gibt, wobei $\mathfrak{n}_{h,r}(k) = \{n_{h,r}(k), \ldots, n_{h,r}(k)\}$ ist. Wir nennen $\mathfrak{A}$ eine zu $\mathfrak{Q}_r(\mathfrak{n}_{h,r}(k))$ gehörige extremale Abschnittsbasis.

8. Neben einigen ganz speziellen Werten kennt man für $n_{h,r}(k)$ Abschätzungen, die man mit Hilfe des kartesischen Produktes gewinnt. So gilt (vgl. [3])

$$n_{h,r}(k) \geqq n_h\left(\left[\sqrt[r]{k+1}\right] - 1\right) \tag{11}$$

und unter Benutzung von (2) bis (4)

$$n_{h,r}(k) > \frac{\left(\left[\sqrt[r]{k+1}\right] - 1\right)^h}{h^h},$$

also für $h \geqq 2$ und genügend große k

$$n_{h,r}(k) > \frac{\sqrt[r]{k^h}}{h^h} - C_h \sqrt{k^{h-1}} \tag{12}$$

mit einer Konstanten C_h.

Wir wollen hier diese Abschätzung verbessern zu

$$n_{h,r}(k) > \sqrt[r]{\frac{k^h}{h^h}} - h \sqrt[r]{\frac{k^{h-1}}{h^{h-1}}} \tag{13}$$

für $h \geqq 2$, $r \geqq 1$ und genügend große k.

Für $r = 1$ ist (13) nicht so gut wie die in Teil I entwickelten Abschätzungen für $n_h(k)$.

Den Beweis für Ungleichung (13) erbringen wir, indem wir geeignete Abschnittsbasen der Ordnung h konstruieren, die k von $\mathfrak{o}$ verschiedene Elemente enthalten. Dabei verifizieren wir (13) zunächst für die Ordnung $h = 2$ und schließen dann durch Induktion nach h (r fest).

9. *Konstruktion von Abschnittsbasen $\mathfrak{A}_h$ der Ordnung $h (h \geqq 2)$ für $\mathfrak{Q}_r(\mathfrak{n})$.* Sei $\mathfrak{A}_{h-1}$ eine Abschnittsbasis der Ordnung $h - 1$ für $\mathfrak{Q}_r(N_{h-1}, \ldots, N_{h-1})$ und $\mathfrak{A}^*_{h-1}$ die Menge aller Vektoren $\mathfrak{z} = \{z_1, \ldots, z_r\} \neq \mathfrak{o}$ mit $z_\varrho \equiv 0 \pmod{N_{h-1} + 1}$, $|z_\varrho| \leqq sN_{h-1} + s$.

---

[3]) Wir können $\mathfrak{Q}_r(\mathfrak{n})$ auch als kartesisches Produkt schreiben:

$$\mathfrak{Q}_r(\mathfrak{n}) = [0, n] \times \cdots \times [0, n].$$

[4]) Wir brauchen diese Definition nicht in der in [3] ausgesprochenen Allgemeinheit, da wir hier nur r-dimensionale Würfel betrachten.

Dann bildet $\mathfrak{A}_h = \mathfrak{A}_{h-1} \cup \mathfrak{A}^*_{h-1}$ eine Abschnittsbasis der Ordnung h für $\mathfrak{D}_r(N_h, \ldots, N_h)$ mit

$$(14) \qquad N_h = (s+1)\, N_{h-1} + s = (s+1)\,(N_{h-1}+1) - 1.$$

Beweis der Basiseigenschaft von $\mathfrak{A}_h$. Ist $\mathfrak{z} = \{z_1, \ldots, z_r\} \in \mathfrak{D}_r(N_h, \ldots, N_h)$, so hat jede Komponente z_ϱ eine Darstellung

$$z_\varrho = \alpha_\varrho (N_{h-1}+1) + q_\varrho$$

mit $0 \leqq \alpha_\varrho \leqq s$ und $0 \leqq q_\varrho \leqq N_{h-1}$. Also gilt

$$\mathfrak{z} = \mathfrak{a} + \mathfrak{q}$$

mit $\mathfrak{a} = \{\alpha_1(N_{h-1}+1), \ldots, \alpha_r(N_{h-1}+1)\} \in \mathfrak{A}^*_{h-1}$ und $\mathfrak{q} = \{q_1, \ldots, q_r\} \in \mathfrak{D}_r(N_{h-1}, \ldots, N_{h-1})$. Nach Voraussetzung läßt sich demnach $\mathfrak{q}$ als Summe von $h-1$ Summanden aus $\mathfrak{A}_{h-1}$ darstellen, womit die Basiseigenschaft von $\mathfrak{A}_h$ gezeigt ist.

Für die Anzahl k der von $\mathfrak{o}$ verschiedenen Elemente in $\mathfrak{A}_h$ haben wir also

$$(15) \qquad k = A_h(N_h, \ldots, N_h) = A_{h-1}(N_{h-1}, \ldots, N_{h-1}) + (s+1)^r - 1,$$

denn die Anzahl der Variationen p-ter Klasse von n Elementen mit Wiederholung ist n^p.

10. Ist nun k vorgegeben, so wollen wir $A_{h-1}(N_{h-1}, \ldots, N_{h-1}) = u$ (und damit auch s) so wählen, daß N_h möglichst groß wird. Im Fall $h = 2$ setzen wir dazu $\mathfrak{A}_{h-1}$ als die Gesamtheit aller Vektoren $\mathfrak{z} = \{z_1, \ldots, z_r\}$ mit $0 \leqq z_\varrho \leqq \left[\sqrt[r]{\frac{k}{2}}\right] - 1$ $(\varrho = 1, \ldots, r)$ an. Folglich wird $N_{h-1} = \left[\sqrt[r]{\frac{k}{2}}\right] - 1$, die Anzahl $A_{h-1}(N_{h-1}, \ldots, N_{h-1}) = \left[\sqrt[r]{\frac{k}{2}}\right]^r - 1$ und somit $s + 1 \geqq \left[\sqrt[r]{\frac{k}{2} + 2}\right]$. Für N_2 erhalten wir aus (14) also die Abschätzungen

$$N_2 \geqq \left[\sqrt[r]{\frac{k}{2}+2}\right] \cdot \left[\sqrt[r]{\frac{k}{2}}\right] - 1 > \left(\sqrt[r]{\frac{k}{2}+2} - 1\right)\left(\sqrt[r]{\frac{k}{2}} - 1\right) - 1$$
$$> \sqrt[r]{\frac{k^2}{4} + \frac{(4-\varepsilon)\,k}{4}} - 2\sqrt[r]{\frac{k}{2}}$$

für beliebiges $\varepsilon > 0$ und alle $k \geqq k_0(\varepsilon)$, oder etwas abgeschwächt

$$n_{2,r}(k) \geqq N_2 > \sqrt[r]{\frac{k^2}{4}} - 2\sqrt[r]{\frac{k}{2}}.$$

Sei die Ungleichung

$$(16) \qquad n_{h,r}(k) \geqq N_h \geqq \varphi_h(k) > \sqrt[r]{\frac{k^h}{h^h}} - h\sqrt[r]{\frac{k^{h-1}}{h^{h-1}}}$$

schon für $h-1$ an Stelle von h $(h \geqq 3)$ und alle genügend großen k bewiesen; mit $A_{h-1}(N_{h-1}, \ldots, N_{h-1}) = u$ folgt also $N_{h-1} \geqq \varphi_{h-1}(u)$ für genügend großes u. Wir wählen $u = \left[\frac{k(h-1)}{h}\right]$, was wegen (15) $s + 1 \geqq [\sqrt[r]{k-u+1}] > \sqrt[r]{\frac{k}{h}+1} - 1$ nach sich zieht. Also haben wir für genügend große k

$$N_h \geqq \left[\sqrt[r]{k - \left[\frac{k(h-1)}{h}\right] + 1}\right]\left(\varphi_{h-1}\left(\left[\frac{k(h-1)}{h}\right]\right) + 1\right) - 1$$

$$> \left[\sqrt[r]{\frac{k}{h} + 1}\right] \varphi_{h-1}\left(\left[\frac{k(h-1)}{h}\right]\right)$$

$$> \left(\sqrt[r]{\frac{k}{h} + 1} - 1\right) \varphi_{h-1}\left(\left[\frac{k(h-1)}{h}\right]\right).$$

Da $\left[\frac{k(h-1)}{h}\right] \geqq \frac{k(h-1)}{h} - \frac{h-1}{h} = \frac{(k-1)(h-1)}{h}$ ist, wird mit

$$\varphi_{h-1}(u) > \sqrt[r]{\frac{u^{h-1}}{(h-1)^{h-1}}} - (h-1)\sqrt[r]{\frac{u^{h-2}}{(h-1)^{h-2}}},$$

also

$$N_h > \left(\sqrt[r]{\frac{k}{h} + 1} - 1\right)\left(\sqrt[r]{\frac{(k-1)^{h-1}}{h^{h-1}}} - (h-1)\sqrt[r]{\frac{k^{h-2}}{h^{h-2}}}\right)$$

$$> \sqrt[r]{\frac{(k+h)(k-1)^{h-1}}{h^h}} - (h-1)\sqrt[r]{\frac{k^{h-1}}{h^{h-1}} + \frac{k^{h-2}}{h^{h-2}}} - \sqrt[r]{\frac{(k-1)^{h-1}}{h^{h-1}}} + (h-1)\sqrt[r]{\frac{k^{h-2}}{h^{h-2}}}$$

für genügend große k. Unter Verwendung der in Nr. 11 bewiesenen Hilfssätze 1 und 2 erhalten wir

$$N_h > \sqrt[r]{\frac{k^h}{h^h} + (1-\varepsilon)\frac{k^{h-1}}{h^h}} - (h-1)\sqrt[r]{\frac{k^{h-1}}{h^{h-1}}} - \sqrt[r]{\frac{(k-1)^{h-1}}{h^{h-1}}}$$

für beliebiges $\varepsilon > 0$ und alle $k \geqq k_0(\varepsilon)$ und

$$n_{h,r}(k) \geqq N_h > \sqrt[r]{\frac{k^h}{h^h}} - h\sqrt[r]{\frac{k^{h-1}}{h^{h-1}}} \quad \text{für genügend große } k.$$

11. Wir geben nun den Beweis der in Nr. 10 benutzten Hilfssätze:

Hilfssatz 1. *Seien h und k natürliche Zahlen. Dann gilt*

$$(k+h)(k-1)^{h-1} \geqq k^h + (1-\varepsilon)k^{h-1}$$

mit einem beliebigen $\varepsilon > 0$ für alle $k \geqq k_0(\varepsilon)$.

Beweis. Für $h = 1$ ist die Behauptung richtig, wie man sofort bestätigt. Wir schließen induktiv. Sei schon

$$(k+h-1)(k-1)^{h-2} \geqq k^{h-1} + (1-\varepsilon)k^{h-2}$$

für $h \geqq 2$, $\varepsilon > 0$ und für alle $k \geqq k_0(\varepsilon)$ bewiesen. Dann erhalten wir daraus durch Multiplikation mit k

$$(k+h-1)k(k-1)^{h-2} \geqq k^h + (1-\varepsilon)k^{h-1};$$

es ist aber $(k+h-1)k = (k+h)(k-1) + h$, woraus

$$(k+h)(k-1)^{h-1} + h(k-1)^{h-2} \geqq k^h + (1-\varepsilon)k^{h-1}$$

und

$$(k+h)(k-1)^{h-1} \geqq k^h + (1-\varepsilon)k^{h-1}$$

mit $\varepsilon > 0$ und für alle $k \geqq k_0^*(\varepsilon)$ folgt.

Hilfssatz 2. $\sqrt[r]{a+b} - \sqrt[r]{b} \leqq \sqrt[r]{a}$ $(a, b \geqq 0;$ *r natürliche Zahl*$)$.

Beweis. Aus dem binomischen Satz folgt $\sqrt[r]{a+b} \leqq \sqrt[r]{a} + \sqrt[r]{b}$.

Literatur.

[1] *H. Rohrbach*, Ein Beitrag zur additiven Zahlentheorie. Math. Z. **42** (1937), 1—30.
[2] *A. Stöhr*, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I. J. reine angew. Math. **194** (1955), 40—65.
[3] *E. Härtter*, Basen für Gitterpunktmengen. J. reine angew. Math. **202** (1959), 153—170.

Eingegangen 20. Oktober 1959.

Der individuelle Ergodensatz in der Theorie der Gleichverteilung mod 1.

Von *Johann Cigler* in Mainz.

Die vorliegende Arbeit hat das Ziel, einige Resultate aus der Theorie der Gleichverteilung, die im wesentlichen von I. I. Schapiro-Pjatezkij und A. G. Postnikow erzielt wurden, auf rein ergodentheoretischem Wege neu zu beweisen und zu verallgemeinern. Im ersten Abschnitt werden die allgemeinen Sätze aus der Ergodentheorie abgeleitet, die diesen Resultaten zugrunde liegen. Sie sind eine direkte Verallgemeinerung der Methode und Ergebnisse von [14]. In den folgenden Abschnitten werden Anwendungen auf die Theorie der Gleichverteilung behandelt. Die Arbeit schließt mit einigen Sätzen über vollständig gleichverteilte Folgen und normale Zahlen, deren Beweis durch Resultate von E. Hlawka ermöglicht wurde.

1. Es sei X ein kompakter Raum mit abzählbarer Basis. $C(X)$ sei der Raum der reellen stetigen Funktionen $f(x)$ auf X mit der Norm $\| f \| = \sup_{x \in X} | f(x) |$. Unter $M(X)$ verstehen wir die Menge aller positiven normierten Maße $\mu(f)$ auf $C(X)$, d. h. die Menge aller linearen stetigen Funktionale μ, für die $\mu(f) \geqq 0$ für jede nichtnegative Funktion $f(x)$ und $\mu(1) = 1$ ist. Wir führen in $M(X)$ die schwache Topologie ein und setzen $\| \mu \| = \sup_{\|f\| \leqq 1} | \mu(f) |$. Den Raum aller μ-integrierbaren Funktionen nennen wir $L_\mu(X)$. Sei T eine Transformation, die den Raum X in sich überführt.

Unter I_T verstehen wir die Menge aller Maße $\mu \in M(X)$ mit $\mu(f(x)) = \mu(f(Tx))$ für alle Funktionen $f(x)$ aus $L_\mu(X)$. Wir nennen ein solches *Maß invariant bezüglich* T. Die Menge I_T ist möglicherweise leer. Wir betrachten in der Folge nur solche Transformationen T, für die dieser Fall nicht eintritt.

Es sei E_T die Menge aller Maße $\mu \in I_T$, für die T ergodisch ist, d. h. für die jede μ-meßbare invariante Funktion für μ-fast alle x konstant ist. Eine *Funktion* $f(x)$ heißt *invariant* (bezüglich T), wenn $f(Tx) = f(x)$ gilt mit Ausnahme einer Menge vom μ-Maß Null. Ein Maß $\mu \in E_T$ wollen wir der Kürze halber ergodisch bezüglich T nennen.

Sind zwei Maße μ und ν gegeben und ist $\nu(f) = 0$ jedesmal, wenn $\mu(f) = 0$ ist für eine beliebige nichtnegative Funktion f, dann nennen wir ν *totalstetig* bezüglich μ, in Zeichen $\nu \ll \mu$.

Es gelten dann die folgenden Sätze:

Individueller Ergodensatz. *Ist $\mu \in I_T$ und $f \in L_\mu(X)$, dann ist für μ-fast alle $x \in X$ die Folge $\frac{1}{n+1} \sum_{j=0}^{n} f(T^j x)$ konvergent. Die Grenzfunktion f^* liegt in $L_\mu(X)$ und ist invariant.*

Ist $\mu \in E_T$ und $f \in L_\mu(X)$, dann ist für μ-fast alle $x \in X$

$$\lim_{n \to \infty} \frac{1}{n+1} \sum_{j=0}^{n} f(T^j x) = \mu(f). \tag{1}$$

Für den Beweis verweisen wir auf [1].

Satz 1[1]. *Ist $\nu \in I_T$, $\mu \in E_T$ und $\nu \ll \mu$, dann ist $\nu = \mu$. In Worten: Ist μ ergodisch bezüglich T, dann gibt es kein invariantes Maß $\nu \neq \mu$, das totalstetig bezüglich μ ist.*

Beweis. Wir setzen $f(T^i x) = f_i(x)$, $f_0 = f$ und bezeichnen die Menge aller x, für die (1) nicht erfüllt ist, mit A. Dann ist $\mu(A) = 0$ und daher auch $\nu(A) = 0$. Aus der Invarianz von ν folgt $\nu(f_0) = \nu(f_1) = \cdots = \nu(f_n) = \cdots$. Mit der Bezeichnung

$$F_n = \frac{1}{n+1}\left(f_0(x) + \cdots + f_n(x)\right)$$

ist also

$$\nu(f) = \nu(F_n) = \lim_{n\to\infty} \nu(F_n).$$

Aus der Ungleichung $\left\| \frac{f_0 + f_1 + \cdots + f_n}{n+1} \right\| \leqq \| f \|$ für jedes $f \in C(X)$ ergibt sich, daß $\lim\limits_{n\to\infty} \nu(F_n) = \nu\left(\lim\limits_{n\to\infty} F_n\right)$ ist.

Folglich ist $\nu(f) = \nu\left(\lim\limits_{n\to\infty} F_n\right) = \nu(\mu(f)) = \mu(f)$; w. z. b. w.

Satz 2. 1) *Die Menge I_T ist konvex und abgeschlossen.*

2) *E_T ist die Menge der Extremalmaße von I_T.*

3) *Die Menge I_T ist die konvexe Hülle von E_T.*

Beweis. 1) Ist $\mu(f) = \mu(f_1)$, $\nu(f) = \nu(f_1)$, dann ist auch $(\lambda_1\mu + \lambda_2\nu)(f) = (\lambda_1\mu + \lambda_2\nu)(f_1)$, wenn $0 \leqq \lambda_i \leqq 1$ und $\lambda_1 + \lambda_2 = 1$ gilt, womit die Konvexität bewiesen ist. Um zu zeigen, daß I_T abgeschlossen ist, genügt es nachzuweisen, daß jede konvergente Folge von invarianten Maßen gegen ein invariantes Maß strebt. Die Folge μ_n strebt gegen μ, wenn für jede Funktion $f(x)$ aus $C(X)$ die Folge $\mu_n(f)$ gegen $\mu(f)$ strebt. Nun ist für $n = 1, 2, 3, \ldots$ wegen der Invarianz $\mu_n(f) = \mu_n(f_1)$, also gilt auch $\mu(f) = \mu(f_1)$.

2) Unter einem Extremalmaß $\mu \in I_T$ verstehen wir ein Maß, das sich nicht in der Form $\mu = \lambda_1\mu_1 + \lambda_2\mu_2$, $\mu_i \in I_T$, $\mu_1 \neq \mu_2$, $0 < \lambda_i < 1$, darstellen läßt. Ist μ kein Extremalmaß, dann nennen wir es zerlegbar (dieser Begriff bezieht sich natürlich auf I_T). Wir führen den Beweis in zwei Schritten:

a) Ist μ ergodisch, dann ist es Extremalmaß.

Wir nehmen an, es wäre kein Extremalmaß. Dann gibt es eine Darstellung $\mu = \lambda_1\mu_1 + \lambda_2\mu_2$, $\mu_i \in I_T$, $\mu_1 \neq \mu_2$, $0 < \lambda_i < 1$, $\Sigma\, \lambda_i = 1$. Es bedeute jetzt f eine nichtnegative Funktion. Ist $\mu(f) = 0$, d. h. $\lambda_1\mu_1(f) + \lambda_2\mu_2(f) = 0$, so ist $\mu_1(f) = 0$, $\mu_2(f) = 0$. Es ist also $\mu_1 \ll \mu$, $\mu_2 \ll \mu$. Daraus folgt nach Satz 1 der Widerspruch

$$\mu_1 = \mu_2 = \mu.$$

b) Ist μ unzerlegbar, dann ist es ergodisch.

Wäre es nämlich nicht ergodisch, dann gäbe es zwei Mengen B_1 und B_2 mit $T^{-1}B_1 = B_1$, $T^{-1}B_2 = B_2$, ($T^{-1}B$ = vollständiges Urbild von B). Dann definieren wir zwei invariante Maße μ_1 und μ_2 folgendermaßen:

Wir setzen

$$\mu_1 = \begin{cases} \dfrac{\mu}{\mu(B_1)} & \text{auf } B_1, \\ 0 & \text{auf } B_2, \end{cases} \qquad \mu_2 = \begin{cases} 0 & \text{auf } B_1 \\ \dfrac{\mu}{\mu(B_2)} & \text{auf } B_2. \end{cases}$$

Es wäre somit $\mu = \mu(B_1)\,\mu_1 + \mu(B_2)\,\mu_2$, und das widerspricht der Voraussetzung.

[1]) Dieser Satz stammt von A. G. Postnikow und I. I. Pjatezkij [12].

3) Die Menge I_T ist konvex und als abgeschlossene Teilmenge der (in der schwachen Topologie) kompakten Menge $M(X)$ selbst kompakt. Daraus ergibt sich nach dem Satz von Krein-Milman ([7], S. 62), daß E_T nicht leer und I_T die konvexe Hülle ihrer Extremalmaße ist.

Jetzt kann Satz 1 verschärft werden zu

Satz 3. *Das Maß $\mu \in I_T$ ist dann und nur dann ergodisch, wenn es kein invariantes Maß $\nu \neq \mu$ gibt, das totalstetig bezüglich μ ist.*

Beweis. Es ist nur noch zu zeigen, daß μ ergodisch ist, wenn die Relation $\nu \ll \mu$ in I_T nur für $\nu = \mu$ erfüllbar ist. Angenommen, es wäre nicht ergodisch, dann gäbe es eine Darstellung

$$\mu = \lambda_1 \mu_1 + \lambda_2 \mu_2, \ \mu_1 \neq \mu_2, \ \mu_i \in I_T, \ 0 < \lambda_i < 1.$$

Es wäre dann aber jedes ν der Gestalt $\nu = \bar{\lambda}_1 \mu_1 + \bar{\lambda}_2 \mu_2$ totalstetig bezüglich μ, was der Voraussetzung widerspricht.

Wir definieren nun den für das Folgende grundlegenden Begriff des Verteilungsmaßes einer Folge.

Definition. Ein Maß $\mu \in M(X)$ heißt *Verteilungsmaß einer Folge* $\{x_n\}$ von Punkten aus X, wenn

$$\lim_{n \to \infty} \frac{1}{n+1} \left(f(x_1) + f(x_2) + \cdots + f(x_n)\right) = \mu(f)$$

für jedes $f \in C(X)$ gilt.

Die Menge der Verteilungsmaße aller Folgen der Form $\{T^n x\}$ bezeichnen wir mit V_T.

Satz 4. *Ist V_T konvex und abgeschlossen, dann ist $V_T = I_T$.*

Beweis. Es genügt zu zeigen, daß die Menge der Extremalmaße von V_T mit E_T übereinstimmt. Das läßt sich genau so wie bei Satz 2, 2) beweisen. Daß jedes ergodische Maß auch Verteilungsmaß ist, ergibt sich unmittelbar aus dem individuellen Ergodensatz.

Satz 5. *Es sei F eine Menge von nichtnegativen Funktionen f mit der Eigenschaft, daß sich jede stetige Funktion auf X durch Linearkomposita von Funktionen aus F approximieren läßt. Gibt es nun ein Maß $\mu \in E_T$ und eine Konstante $c \geqq 1$, so daß die Relation*

$$\overline{\lim_{n \to \infty}} \frac{1}{n+1} \left(f(x) + f(Tx) + \cdots + f(T^n x)\right) \leqq c\mu(f) \tag{2}$$

für ein festes $x \in X$ und jedes $f \in F$ erfüllt ist, dann besitzt die Folge $\{T^n x\}$ das Verteilungsmaß μ.

Beweis. Es ist folgendes zu zeigen: Aus (2) folgt, daß $\lim\limits_{n \to \infty} \frac{1}{n+1} \sum\limits_{j=0}^{n} f(T^j x)$ existiert und für jedes $f \in F$ gleich $\mu(f)$ ist. Denn ist das gezeigt, so ergibt sich die Behauptung des Satzes durch Approximation.

Es sei $p_n(f) = \frac{1}{n+1} \sum\limits_{j=0}^{n} f(T^j x)$. Dann ist $p_n(f) = p_n(f_1) + \frac{2\vartheta \, \| f \|}{n+1}$. Die Menge der Häufungsmaße der Folge $p_n(f)$ ist relativ kompakt. Sei π ein solches Häufungsmaß. Es gibt also eine Teilfolge p_{n_k} mit $\lim p_{n_k}(f) = \pi(f)$ für jedes $f \in F$ (vgl. [3]). Aus der Voraussetzung folgt $\pi(f) \leqq c\mu(f)$. Ferner ist $\pi(f) = \pi(f_1)$. Es ist also $\pi \in I_T$, $\pi \ll \mu$, und da μ ergodisch ist, folgt $\pi = \mu$. Es ist somit jedes Häufungsmaß der Folge

$$\frac{1}{n+1} (f_0 + f_1 + \cdots + f_n)$$

gleich μ. Daher existiert $\lim p_n(f)$ und ist gleich μ.

Ist V_T konvex, dann gilt auch die Umkehrung zu Satz 5, also der

Satz 6. *Es sei V_T konvex und F eine Menge mit den in Satz 5 definierten Eigenschaften. Ist für das Maß $\mu \in I_T$ die Relation (2) für alle $f \in F$ und eine geeignete Konstante $c > 1$ hinreichend dafür, daß μ Verteilungsmaß der Folge $\{T^n x\}$ ist, so ist μ ergodisch.*

Beweis. Wir nehmen an, μ wäre nicht ergodisch, d. h. $\mu = \lambda_1 \mu_1 + \lambda_2 \mu_2$, $0 < \lambda_i < 1$. Da V_T konvex ist, ist auch jedes Maß der Gestalt $\bar{\lambda}_1 \mu_1 + \bar{\lambda}_2 \mu_2$ mit $\bar{\lambda}_1 \neq \lambda_1$ ein Verteilungsmaß. Ist $\bar{\lambda}_1 \mu_1 + \bar{\lambda}_2 \mu_2 \leqq c(\lambda_1 \mu_1 + \lambda_2 \mu_2)$, so folgt $\bar{\lambda}_1 \leqq c\lambda_1$, $\bar{\lambda}_2 \leqq c\lambda_2$. Diese Ungleichungen können aber durch unendlich viele $\bar{\lambda}_i$ erfüllt werden. Das ist ein Widerspruch zur Voraussetzung des Satzes.

Eine unmittelbare Folgerung von Satz 5 ist der

Satz 7. *Ist*[2]) *$\mu \in E_{T^k}$ für eine natürliche Zahl k und ist das Verteilungsmaß von $\{T^n x\}$ gleich μ für ein $x \in X$, dann besitzt auch jede der Folgen $\{T^{kn+l} x\}$ $(l = 0, 1, \ldots, k-1)$ das Verteilungsmaß μ.*

Beweis. Es existiert stets eine Menge F mit den in Satz 5 geforderten Eigenschaften. Für jedes $f \in F$ gilt

$$f(T^l x) + f(T^{k+l} x) + \cdots + f(T^{k(n-1)+l} x) \leqq f(x) + f(Tx) + \cdots + f(T^{kn} x).$$

Folglich ist $\overline{\lim\limits_{n\to\infty}} \frac{1}{n} \sum\limits_{j=0}^{n-1} f(T^{kj+l} x) \leqq \overline{\lim\limits_{n\to\infty}}\, k \cdot \frac{1}{kn} \sum\limits_{j=0}^{kn} f(T^j x) = k \cdot \mu(f)$. Daraus folgt nach Satz 5 die Behauptung des Satzes.

Bemerkung. Wir nannten ein Maß μ Verteilungsmaß einer Folge $\{x_n\}$, wenn

$$\text{(a)} \qquad \lim_{n\to\infty} \mu_n(f) = \lim_{n\to\infty} \frac{1}{n} \left(f(x_1) + f(x_2) + \cdots + f(x_n)\right) = \mu(f)$$

für jedes $f \in C(X)$ gilt. In den folgenden Abschnitten wird es oft nötig sein,

$$\text{(b)} \qquad \lim_{n\to\infty} \mu_n(B) = \mu(B)$$

für alle Borelschen Mengen B zu betrachten. Es erhebt sich nun die Frage, unter welchen Bedingungen (a) und (b) gleichzeitig erfüllt ist. Diese Frage wurde von Stromberg [15] behandelt. Eine grundlegende Rolle spielt dabei der Begriff der Stetigkeitsmenge.

Definition. Eine Borelsche Menge B heißt *Stetigkeitsmenge* für ein Maß μ, wenn der Rand von B das μ-Maß Null besitzt,

Mit dieser Bezeichnung gilt das

Lemma (Stromberg [15]). *Es ist $\lim\limits_{n\to\infty} \mu_n(f) = \mu(f)$ für jedes $f \in C(X)$ genau dann, wenn $\lim\limits_{n\to\infty} \mu_n(B) = \mu(B)$ für jede Stetigkeitsmenge B gilt.*

Ist für ein Maß μ jede Borelsche Menge B Stetigkeitsmenge, so nennen wir *μ stetig*. Wir werden uns im folgenden hauptsächlich auf stetige Maße beschränken und auch von den Mengen E_T, I_T und V_T voraussetzen, daß sie aus allen stetigen Maßen mit den entsprechenden Eigenschaften bestehen. Die Sätze aus Abschnitt 1, insbesondere Satz 2 und Satz 4 bleiben auch in diesem Fall richtig. Unter den gemachten Voraussetzungen sind dann natürlich die Definitionen (a) und (b) äquivalent.

---

[2]) Aus $\mu \in E_T$ folgt nicht immer $\mu \in E_{T^k}$.

Beispiel: Sei $Tx = 2x \pmod 1$ und μ das Maß, das den Punkten $1/3$, $2/3$ das Maß $1/2$, den übrigen Punkten von $(0, 1)$ das Maß 0 zuordnet. Dann ist T ergodisch bezüglich des Maßes μ, jedoch nicht T^2. Denn $T^2 x = 4x \pmod 1$ läßt jeden der Punkte $1/3$, $2/3$ für sich invariant.

2. Wir wollen nun die obigen Sätze auf den Fall anwenden, daß X die k-dimensionale Torusgruppe X_k ist ($k \geqq 1$), d. h. daß X isomorph zur additiven Gruppe aller k-tupel reeller Zahlen mod 1 ist.

Zuerst einige Bemerkungen über Matrizen. Eine Matrix $A = (a_{ij})$ heißt *ganzzahlig*, wenn alle a_{ij} ganz rational sind. Unter der Norm $\| A \|$ einer Matrix verstehen wir die Hilbert-Norm: $\| A \| = \sup\limits_{|\mathfrak{x}| \leq 1} | A\mathfrak{x} |$. Man zeigt leicht, daß $\| A \|^2 = \varrho^2$ ist, wo ϱ^2 der größte Eigenwert der Matrix A^*A ist, wenn A^* die Transponierte bedeutet.

Unter W_k wollen wir im folgenden den k-dimensionalen Einheitswürfel verstehen. Mit $\mathfrak{n} = (n_1, n_2, \ldots, n_k)$ bezeichnen wir einen Gittervektor, d. h. einen Vektor, dessen sämtliche Koordinaten ganze Zahlen sind.

Bekanntlich läßt sich jedes Maß μ auf X_k als Stieltjes-Integral mit einer im wesentlichen eindeutig bestimmten Gewichtsfunktion darstellen. Ist μ ein Verteilungsmaß, so wollen wir die zugehörige Gewichtsfunktion $\mu(\mathfrak{x})$ *Verteilungsfunktion* nennen. Sie ist durch $\mu(\mathfrak{x}) = \mu(\varphi(x_1, \ldots, x_k))$ gegeben, wo $\varphi(x_1, \ldots, x_k)$ die charakteristische Funktion des Bereiches $0 \leqq t_i \leqq x_i$ $(i = 1, \ldots, k)$ bedeutet.

Mit diesen Bezeichnungen gilt der

Satz 8[3]. *Ist A eine ganzzahlige k-reihige Matrix, $| \operatorname{Det} A | > 1$, und gibt es eine natürliche Zahl l mit $\| A^{-l} \| < 1$, dann ist dafür, daß die stetige Funktion $\sigma(\mathfrak{x}) = \sigma(x_1, \ldots, x_k)$ Verteilungsfunktion einer Folge $\{A^n\mathfrak{x}\}$ (mod 1) ist, die folgende Invarianzbedingung notwendig und hinreichend:*

$$\int\limits_{X_k} f(\mathfrak{x})\, d\sigma(\mathfrak{x}) = \int\limits_{X_k} f(A\mathfrak{x})\, d\sigma(\mathfrak{x}) \text{ für jedes } f \in C(X_k). \tag{3}$$

Beweis. Es genügt zu zeigen, daß V_A konvex und abgeschlossen ist. Ist $\| A^{-l} \| < 1$, dann ist wegen $| A^{-l\nu}\mathfrak{x} | \leqq \| A^{-l} \|^\nu \cdot |\mathfrak{x}|$ die Folge $| A^{-n}\mathfrak{x} |$ eine Nullfolge. Es strebt daher auch der Durchmesser der Parallelepipede $A^{-n}W_k$ gegen Null, wobei $A^{-n}W_k$ die Menge $A^{-n}\mathfrak{x}$ mit $\mathfrak{x} \in W_k$ bedeuten soll. Offenbar ist $A^{-1}W_k$ ein Parallelepiped vom Volumen d^{-1}, wenn $d = | \operatorname{Det} A |$ gesetzt wurde. Man zeigt nun leicht, daß jedes Parallelepiped der Form $A^{-1}(W_k + \mathfrak{n})$ aus lauter mod 1 inkongruenten Punkten besteht und daß es genau d mod 1 inäquivalente Parallelepipede dieser Gestalt gibt. Wir nehmen d solche Parallelepipede, numerieren sie in beliebiger Reihenfolge und bilden ihre Bilder mod 1, die ganz in W_k liegen: $B_0, B_1, \ldots, B_{d-1}$. Wir bezeichnen die Abbildung, die W_k in B_i überführt, mit T_i. Offenbar ist $AB_i = W_k$ mod 1. Weiter definieren wir induktiv

$$T_j B_i = B_j B_i, \quad T_{i_1} B_{i_2} B_{i_3} \cdots B_{i_n} = B_{i_1} B_{i_2} \cdots B_{i_n}.$$

Liegt ein Punkt $\mathfrak{x}$ in jeder der Mengen $B_{i_1}, B_{i_1}B_{i_2}, B_{i_1}B_{i_2}B_{i_3}, \ldots$, so können wir ihn symbolisch als $\mathfrak{x} = B_{i_1}B_{i_2}B_{i_3} \cdots$ schreiben. Verschiedene Punkte haben dann verschiedene Darstellungen, und die Transformation A geht über in eine Translation der Indizes: $A\mathfrak{x} = B_{i_2}B_{i_3}B_{i_4} \cdots$.

Unter einer *Zylindermenge* wollen wir eine Menge der Gestalt $B = B_{i_1}B_{i_2}B_{i_3} \cdots$ verstehen, wo endlich viele Indizes i_ν feste Werte besitzen, während die anderen unabhängig voneinander alle Werte $i = 0, 1, \ldots, d-1$ durchlaufen. Die lineare Hülle der charakteristischen Funktionen aller Zylindermengen umfaßt die stetigen Funktionen. Man kann sich also beim Beweis des Satzes darauf beschränken, die Grenzwerte $\lim\limits_{n \to \infty} \frac{1}{n+1} \sum\limits_{\nu=0}^{n} f(A^\nu\mathfrak{x})$ zu betrachten, wo f die charakteristische Funktion einer Zylindermenge ist. Man zeigt nun wörtlich wie bei I. I. Schapiro-Pjatezkij [14], daß die Menge der Verteilungsfunktionen konvex und abgeschlossen ist. Damit ist Satz 8 bewiesen.

[3]) Im Fall $k = 1$ wurde der entsprechende Satz von I. I. Schapiro-Pjatezkij [14] gezeigt.

Satz 9. *Erfüllt A die Bedingungen von Satz 8, dann ist die Transformation $A\mathfrak{x}$ (mod 1) ergodisch bezüglich des Lebesgueschen Maßes.*

Beweis. Der Beweis verläuft analog zu [1], S. 29.

Bemerkung. Satz 9 bleibt richtig, wenn außer der Ganzzahligkeit von A nur vorausgesetzt wird, daß $d \geqq 1$ und kein Eigenwert eine Einheitswurzel ist (vgl. [13]).

Aus Satz 5 folgt sofort der

Satz 10. *Erfüllt A die Bedingungen von Satz 8 und ist μ stetig und ergodisch bezüglich A, so hat die Folge $\{A^n\mathfrak{x}\}$ genau dann die Verteilungsfunktion $\mu(\mathfrak{x})$, wenn für jeden Würfel $v \leqq W_k$ mit achsenparallelen Kanten $\overline{\lim\limits_{p\to\infty}} \frac{N_p(v)}{p} \leqq c\mu(v)$ ist. Hier bedeutet $c \geqq 1$ eine Konstante und $N_p(v)$ die Anzahl der Punkte $\{A^\nu\mathfrak{x}\}$, $0 \leqq \nu < p$, die in v liegen.*

Beweis. Wie man leicht feststellt, kann man mit den charakteristischen Funktionen dieser Würfel jede stetige Funktion approximieren.

Aus der Bemerkung zu Satz 9 folgert man den

Satz 11[4]. *Ist A ganzzahlig, $|\operatorname{Det} A| \geqq 1$, und ist kein Eigenwert eine Einheitswurzel, dann ist die Folge $\{A^n\mathfrak{x}\}$ genau dann gleichverteilt, wenn für jeden beliebigen Würfel v vom Volumen $|v|$ mit achsenparallelen Kanten, der ganz im Einheitswürfel liegt,*

$$\overline{\lim_{p\to\infty}} \frac{N_p(v)}{p} \leqq c\,|v|$$

ist.

Aus Satz 9 und Satz 7 liest man unmittelbar den folgenden Satz ab:

Satz 12. *Erfüllt A die Bedingungen von Satz 9 und ist $\{A^n\mathfrak{x}\}$ gleichverteilt, dann auch die Folge $\{A^{kn+l}\mathfrak{x}\}$ für jede natürliche Zahl k und $l = 0, 1, \ldots, k-1$.*

3. Wir wählen jetzt als X den *Jessenschen Torusraum* X_∞ (siehe [5]). Man kann X_∞ darstellen als Menge aller Folgen $x = \{x_n\}$ mit $0 \leqq x_n < 1$. Sind $A_1, A_2, \ldots$ Teilmengen von $[0, 1)$, so verstehen wir unter $A = \{A_1, A_2, \ldots, A_n, \ldots\}$ die Menge aller Folgen $a = \{a_n\}$, bei denen $a_i \in A_i$ für $i = 1, 2, \ldots$ gilt. Unter einem Intervall B verstehen wir eine Menge $B = \{B_1, B_2, \ldots, B_n, \ldots\}$, wo endlich viele B_n offene Intervalle in $[0, 1)$ und die übrigen B_n ganz $[0, 1)$ bedeuten sollen. Ist μ ein normiertes Maß auf $[0, 1)$, so wollen wir mit μ_∞ das Maß auf X_∞ bezeichnen, das jedem Intervall B den Wert $\mu_\infty(B) = \prod\limits_{n=1}^{\infty} \mu(B_n)$ zuordnet. (Das rechts stehende Produkt ist nur formal unendlich, da ja von einer Stelle ab $\mu(B_n) = \mu([0, 1)) = 1$ ist.)

Setzt man $T\{x_1, x_2, \ldots, x_n, \ldots\} = \{x_2, x_3, \ldots, x_{n+1}, \ldots\}$, so ist die Transformation T für jedes μ_∞ ergodisch (siehe [1], S. 29). Für jede Funktion $f \in C(X_\infty)$ gilt also

$$\lim_{n\to\infty} \frac{1}{n+1}\left(f(x) + f(Tx) + \cdots + f(T^n x)\right) = \mu_\infty(f) \tag{4}$$

für μ_∞-fast alle Folgen $x \in X_\infty$.

Gilt (4), so sagen wir, die Folge $x = \{x_n\}$ sei *vollständig verteilt* zur Verteilungsfunktion μ. Ist μ das Haarsche Maß auf $[0, 1)$, so nennen wir mit A. G. Postnikow [10] die Folge x *vollständig gleichverteilt.*

---

[4]) Im Eindimensionalen, also für Folgen der Gestalt $\{a^n x\}$, wurde dieser Satz von I. I. Schapiro-Pjatezkij [14] gezeigt. Er wurde dann von A. G. Postnikow [9] auf Folgen der Gestalt $\{(a + bi)^n(x + iy)\}$ verallgemeinert, die in unserer Schreibweise auf Matrizen der Form $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ führen. Die allgemeine Fassung stammt von A. M. Polosujew [8]. Zum Beweis wurde die Vinogradowsche Methode der trigonometrischen Summen verwendet. Satz 10 stammt im eindimensionalen Fall zum Großteil von I. I. Schapiro-Pjatezkij und A. G. Postnikow [11].

Satz 13. *Eine Folge $e = \{e_n\}$ ist genau dann vollständig verteilt zur stetigen Verteilungsfunktion $\mu(x)$, wenn für jedes $k = 1, 2, 3, \ldots$ die Folge der Vektoren $\{(e_n, e_{n+1}, \ldots, e_{n+k-1})\}$ die Verteilungsfunktion $\mu(x_1) \cdot \mu(x_2) \cdots \mu(x_k)$ besitzt*[5]).

Beweis. Ein Maß ist eindeutig bestimmt, wenn es für alle Intervalle B bekannt ist. Die charakteristischen Funktionen der Intervalle sind aber identisch mit den charakteristischen Funktionen von Teilmengen der k-dimensionalen Einheitswürfel ($k = 1, 2, 3, \ldots$).

Aus Satz 5 folgt weiterhin der

Satz 14[6]). *Die Folge $e = \{e_n\}$ ist genau dann vollständig verteilt zur stetigen Verteilungsfunktion $\mu(x)$, wenn bei beliebigem $k \geqq 1$ für jedes Parallelepiped $\Delta_k \subseteqq W_k$ die Ungleichung $\overline{\lim\limits_{p \to \infty}} \dfrac{N_p(\Delta_k)}{p} \leqq c\, \mu_\infty(\Delta_k)$ gilt ($c \geqq 1$, konstant).*

Aus Satz 7 ergibt sich der

Satz 15. *Besitzt die Folge der Vektoren $\{(e_n, e_{n+1}, \ldots, e_{n+k-1})\}$ ($n = 1, 2, \ldots$) für jedes natürliche k die Verteilungsfunktion $\mu(x_1)\, \mu(x_2) \cdots \mu(x_k)$, dann auch die Folge der Vektoren $\{(e_{ln}, e_{ln+1}, \ldots, e_{ln+k-1})\}$ für jedes natürliche l.*

4. Wir bringen nun ein Beispiel, das die Anwendungsmöglichkeiten unserer Sätze illustrieren soll.

Satz 16. *Ist a eine reelle ganzalgebraische Zahl, deren Grad genau k ist, ist $|a| > 1$ und sind die Vektoren $\{(a^n x, a^{n+1} x, \ldots, a^{n+k-1} x)\}$ für ein festes x gleichverteilt, dann ist auch die Folge der Vektoren $\{(a^{ln} x, a^{ln+1} x, \ldots, a^{ln+k-1} x)\}$ für jedes natürliche l gleichverteilt.*

Beweis. Die normierte irreduzible Gleichung, der a genügt, sei $a^k - h_1 a^{k-1} - \cdots - h_k = 0$. Dann ist

$$\begin{pmatrix} a^{n+k} x \\ a^{n+k-1} x \\ \cdot \\ \cdot \\ \cdot \\ a^{n+1} x \end{pmatrix} = \begin{pmatrix} h_1 & h_2 & \cdots & h_{k-1} & h_k \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} a^{n+k-1} x \\ a^{n+k-2} x \\ \cdot \\ \cdot \\ \cdot \\ a^n x \end{pmatrix}.$$

Die hier auftretende Matrix ist ganzzahlig. Der Betrag ihrer Determinante ist $|(-1)^k h_k| \geqq 1$, da k der genaue Grad von a ist. Ihre charakteristische Gleichung ist dieselbe Gleichung, der auch a genügt. Es ist daher wegen $|a| \neq 1$ und der Irreduzibilität der Gleichung kein Eigenwert eine Einheitswurzel. Wir können also Satz 12 anwenden. Damit ist Satz 16 bewiesen.

Es erhebt sich nun die Frage, ob die Voraussetzung von Satz 16 überhaupt realisierbar ist. In dieser Hinsicht beweisen wir den

Satz 17. 1) *Ist $a > 1$ eine algebraische Zahl, deren Grad $\geqq K$ ist, dann ist für fast alle $x \in [0, 1]$ die Folge der Vektoren $(a^n x, a^{n+1} x, \ldots, a^{n+k-1} x)$ gleichverteilt.*

2) *Ist $a > 1$ transzendent, dann ist für fast alle $x \in [0, 1]$ die Folge $\{a^n x\}$ vollständig gleichverteilt.*

Zum Beweis benötigen wir zwei bekannte Hilfssätze.

Hilfssatz 1 (J. F. Koksma [6]). *Ist $f(n, x)$ für jede natürliche Zahl n eine reelle, stetig-differenzierbare Funktion von x auf $[0, 1]$ und ist $f'(n_1, x) - f'(n_2, x)$ für $n_1 \neq n_2$ monoton in $[0, 1]$* und $|f'(n_1, x) - f'(n_2, x)| \geqq K > 0$, *($K$ unabhängig von x, n_1, n_2), dann ist die Folge $\{f(n, x)\}$ für fast alle $x \in [0, 1]$ gleichverteilt* mod 1.

[5]) In der Sprechweise der Wahrscheinlichkeitstheorie heißt das, die Folgen $\{e_n\}, \{e_{n+1}\}, \{e_{n+2}\}, \ldots$ sind paarweise unabhängig.

[6]) Dieser Satz stammt im Spezialfall der vollständig gleichverteilten Folgen von A. G. Postnikow [10].

Hilfssatz 2a (H. Weyl [15]). *Die Folge der Vektoren* $\{(c_n^{(1)}, c_n^{(2)}, \ldots, c_n^{(k)})\}$, $(n = 1, 2, \ldots)$, *ist genau dann gleichverteilt* mod 1, *wenn für jeden Gitterpunkt* $(h_1, h_2, \ldots, h_k) \neq (0, 0, \ldots, 0)$ *die Zahlenfolge* $\{h_1 c_n^{(1)} + \cdots + h_k c_n^{(k)}\}$ *gleichverteilt* mod 1 *ist.*

Für spätere Anwendungen formulieren wir gleich hier den

Hilfssatz 2b. *Die Folge der Vektoren* $\{(c_n^{(1)}, c_n^{(2)}, \ldots, c_n^{(k)})\}$ *besitzt genau dann die Verteilungsfunktion* $\mu(x_1, x_2, \ldots, x_k)$, *wenn für jeden Gitterpunkt* $(h_1, h_2, \ldots, h_k) \neq (0, 0, \ldots, 0)$ *die Folge* $\{h_1 c_n^{(1)} + h_2 c_n^{(2)} + \cdots + h_k c_n^{(k)}\}$ *die Verteilungsfunktion* ν *besitzt, die durch die Relationen*

$$\nu(f) = \int_0^1 \cdots \int_0^1 f(h_1 x_1 + h_2 x_2 + \cdots + h_k x_k)\, d\mu(x_1, \ldots, x_k)$$

für jedes $f \in C(X_k)$ *gegeben ist.*

Der Beweis kann analog zum Beweis von Hilfssatz 2a geführt werden.

Beweis von Satz 17. 1) Nach Hilfssatz 2a braucht nur gezeigt zu werden, daß die Folge $\{h_1 a^n x + h_2 a^{n+1} x + \cdots + h_k a^{n+k-1} x\}$ für fast alle $x \in [0, 1]$ gleichverteilt ist. Wir wenden Hilfssatz 1 mit $f(n, x) = (h_1 + h_2 a + \cdots + h_k a^{k-1})\, a^n x$, d. h. mit $f'(n + l, x) - f'(n, x) = (h_1 + h_2 a + \cdots + h_k a^{k-1})\,(a^l - 1)\, a^n$ an. Diese Funktion erfüllt offenbar alle Forderungen, denn sie ist konstant, und es ist

$$|f'(n + l, x) - f'(n, x)| \geqq (h_1 + h_2 a + \cdots + h_k a^{k-1})\,(a - 1) > 0,$$

weil $a > 1$ und der Grad von a größer als $k - 1$ ist. Damit ist 1) bewiesen. Die Aussage 2) folgt aber unmittelbar aus diesem Beweis; denn ist a transzendent, so sind für jedes natürliche k alle Forderungen von Hilfssatz 1 erfüllt.

5. Wir schließen nun mit einigen Sätzen über vollständig gleichverteilte Folgen und normale Zahlen.

Satz 18. *Ist die Folge* $\{y_n\}$ *vollständig verteilt zum Verteilungsmaß* μ, *wo* μ *durch* $\mu(f) = \int_0^1 f(x)\, p(x)\, dx$ *mit stetigem* $p(x)$ *gegeben ist, dann ist auch die Folge* $\{x_n\}$ *mit* $x_n = y_1 + y_2 + \cdots + y_n$ *gleichverteilt* mod 1.

Zum Beweis benötigen wir einen Spezialfall eines Satzes von E. Hlawka [4], nämlich den

Hilfssatz 3. *Es sei* $p(x) \geqq 0$ *stetig und* $\int_0^1 p(x)\, dx = 1$. *Besitzt die Folge* $\{x_{n+k} - x_n\}$ $(n = 1, 2, 3, \ldots)$ *für jedes natürliche* k *das Verteilungsmaß* ν_k, *gegeben durch*

$$\nu_k(f) = \int_0^1 \cdots \int_0^1 f(x_1 + \cdots + x_k)\, p(x_1) \cdots p(x_k)\, dx_1 \cdots dx_k$$

für jedes $f \in C([0, 1))$, *dann ist die Folge* $\{x_n\}$ *gleichverteilt* mod 1.

Beweis von Satz 18. Da die Folge $\{y_n\}$ vollständig verteilt zum Verteilungsmaß μ ist, besitzt nach Satz 13 und Hilfssatz 2b die Folge $\{y_{n+1} + y_{n+2} + \cdots + y_{n+k}\}$, d. h. die Folge $\{x_{n+k} - x_n\}$ das in Hilfssatz 3 definierte Verteilungsmaß ν_k. Damit folgt nach demselben Hilfssatz, daß die Folge $\{x_n\}$ gleichverteilt ist, und damit die Behauptung von Satz 18.

Ist μ speziell das Haarsche Maß, so kann Satz 18 verschärft werden zum

Satz 19. *Ist die Folge* $\{y_n\}$ *vollständig gleichverteilt, dann auch die Folge* $\{x_n\}$ *mit* $x_n = y_1 + y_2 + \cdots + y_n$.

Beweis. Es ist zu zeigen, daß die Folge der Vektoren

$$\{(y_1 + \cdots + y_n, y_1 + \cdots + y_{n+1}, \ldots, y_1 + \cdots + y_{n+s})\} \quad (n = 1, 2, 3, \ldots)$$

für jedes feste natürliche s gleichverteilt ist, also nach Hilfssatz 2a, daß für jeden Gitterpunkt $(h_1, h_2, \ldots, h_{s+1}) \neq (0, \ldots, 0)$ die Folge $\{z_n\}$ mit

$$z_n = h_1(y_1 + \cdots + y_n) + \cdots + h_{s+1}(y_1 + \cdots + y_{n+s})$$

gleichverteilt mod 1 ist.

Für $z_{n+k} - z_n$ ergibt sich der Ausdruck

$$\begin{aligned} z_{n+k} - z_n &= h_1(y_{n+1} + \cdots + y_{n+k}) + h_2(y_{n+2} + \cdots + y_{n+k+1}) + \cdots \\ &\quad + h_{s+1}(y_{n+s+1} + \cdots + y_{n+s+k}) \\ &= l_1 y_{n+1} + l_2 y_{n+2} + \cdots + l_{s+k} y_{n+s+k}, \end{aligned}$$

wobei die l_i feste ganze Zahlen sind, die nicht alle verschwinden. Da $\{y_n\}$ nach Voraussetzung vollständig gleichverteilt ist, ist also $\{z_{n+k} - z_n\}$ gleichverteilt für jedes natürliche k und somit nach Hilfssatz 3 auch $\{z_n\}$ selbst, womit die Behauptung von Satz 19 bewiesen ist.

Wir zeigen nun die analogen Sätze für normale Zahlen. Zunächst einige Vorbemerkungen:

Bekanntlich kann man jede reelle Zahl x mit $0 \leqq x \leqq 1$ als a-adischen Bruch $x = 0, x_1 x_2 x_3 \ldots$ darstellen, wobei $0 \leqq x_i \leqq a - 1$ gilt. Man kann nun der Zahl x umkehrbar eindeutig die Folge $x = \{x_n\}$ zuordnen. Dabei kann man die x_n als Elemente der additiven Gruppe G_a der Restklassen mod a auffassen.

Ist μ ein Maß auf G_a und setzt man $\mu(\nu) = p_\nu$, so gilt $p_\nu \geqq 0$ und $\sum_{\nu=0}^{a-1} p_\nu = 1$. Speziell für das Haarsche Maß ergibt sich $p_0 = p_1 = \cdots = p_{a-1} = \frac{1}{a}$. Es ist klar, was man unter der Verteilungsfunktion einer Folge von k-tupeln von Elementen aus G_a zu verstehen hat. Bei sinngemäßer Interpretation bleiben alle Definitionen und Sätze des Abschnitts 3 richtig. Wir führen bloß eine andere Terminologie ein: Besitzt die Folge $x = \{x_n\}$ $(x_n \in G_a)$ das Haarsche Maß als Verteilungsmaß, so heißt die Zahl x *einfach normal.* Ist die Folge x vollständig verteilt zum Haarschen Maß, dann heißt x *normal.* Man überzeugt sich leicht davon, daß diese Definitionen von normal und einfach normal mit den üblichen äquivalent sind (vgl. [2]). Ist μ ein normiertes Maß auf G_a, das keiner Restklasse das Maß Null zuordnet, so sagen wir, *μ gehöre zur Menge P.* Ist die Folge x vollständig verteilt zu einem Maß $\mu \in P$, so nennen wir die zugehörige Zahl x *B-normal* (vgl. dazu [11]).

Hilfssatz 2a und 2b bleiben richtig, wenn man die Bedingung

$$(h_1, h_2, \ldots, h_k) \neq (0, \ldots, 0) \text{ durch } (h_1, \ldots, h_k) \not\equiv (0, \ldots, 0) \pmod{a}$$

ersetzt. An Stelle von Hilfssatz 3 tritt Hilfssatz 4, der ebenfalls in weit allgemeinerer Form von E. Hlawka [4] bewiesen wurde.

Hilfssatz 4. *Es sei $\mu \in P$. Besitzt die Folge $\{x_{n+k} - x_n\}$ für jedes natürliche k das Verteilungsmaß ν_k, gegeben durch $\nu_k(f) = \int_{G_a} \cdots \int_{G_a} f(t_1 + \cdots + t_k)\, d\mu(t_1) \cdots d\mu(t_k)$ für jedes $f \in C(G_a)$, dann ist die Folge $\{x_n\}$ gleichverteilt zum Haarschen Maß auf G_a.*

Mit diesen Änderungen überträgt sich der Beweis von Satz 18 und 19 wörtlich auf den Fall der normalen Zahlen und liefert die folgenden Sätze:

Satz 20. *Ist die reelle Zahl $y = 0, y_1 y_2 \cdots y_n \cdots$ B-normal, dann ist die Zahl $x = 0, x_1 x_2 \cdots x_n \cdots$ mit $x_n \equiv y_1 + y_2 + \cdots + y_n \pmod{a}$ einfach normal.*

Satz 21. *Ist die reelle Zahl $y = 0, y_1 y_2 \cdots y_n \cdots$ normal, dann auch die Zahl $x = 0, x_1 x_2 \cdots x_n \cdots$ mit $x_n \equiv y_1 + y_2 + \cdots + y_n \pmod{a}$.*

Literatur.

[1] *P. R. Halmos*, Lectures on Ergodic Theory, Tokio 1956.

[2] *G. H. Hardy* and *E. M. Wright*, An Introduction to the Theory of Numbers, 3. Aufl., Oxford 1956.

[3] *E. Hlawka*, Folgen auf kompakten Räumen, Abh. math. Sem. Hambg. **20** (1956), 223—241.

[4] *E. Hlawka*, Zum Hauptsatz der Theorie der Gleichverteilung, Anz. Österr. Akad. Wiss. Math.-naturwiss. Kl. **94** (1957), 313—317.

[5] *B. Jessen*, The Theory of Integration in a Space of an Infinite Number of Dimensions, Acta math. **63** (1934), 249—323.

[6] *J. F. Koksma*, Ein mengentheoretischer Satz über die Gleichverteilung mod Eins, Comp. math. **2** (1935), 250—258.

[7] *M. A. Neumark*, Normierte Ringe, Moskau 1956 (russ.).

[8] *A. M. Polosujew*, Über die Gleichverteilung eines Systems von Funktionen, das Lösung eines Systems von linearen Differenzengleichungen erster Ordnung ist, Dokl. Akad. Nauk **123** (1958), 405—406 (russ.).

[9] *A. G. Postnikow*, Ein Kriterium für die Gleichverteilung der Exponentialfunktion im Komplexen, Westnik Leningr. Univ. **13** (1957), 81—88 (russ.).

[10] *A. G. Postnikow*, Ein Kriterium für eine vollständig gleichverteilte Folge, Dokl. Akad. Nauk **120** (1958) 973—975 (russ.).

[11] *A. G. Postnikow* und *I. I. Pjatezkij*, Ziffernfolgen, die normal nach Bernoulli sind, Iswest. Akad. Nauk **21** (1957), 501—514 (russ.).

[12] *A. G. Postnikow* und *I. I. Pjatezkij*, Markow-normale Ziffernfolgen und normale Kettenbrüche, Iswest. Akad. Nauk **21** (1957), 729—746 (russ.).

[13] *W. A. Rochlin*, Über Endomorphismen von kompakten abelschen Gruppen, Iswest. Akad. Nauk **13** (1949) 329—340 (russ.).

[14] *I. I. Schapiro-Pjatezkij*, Über die Verteilungsfunktionen der Bruchteile der Exponentialfunktion, Iswest. Akad. Nauk **15** (1951), 49—52 (russ.).

[15] *K. R. Stromberg*, Probabilities on a Compact Group, Thesis, Univ. of Washington 1958.

[16] *H. Weyl*, Über die Gleichverteilung von Zahlen mod. Eins, Math. Ann. **77** (1916), 313—352.

Eingegangen 5. Januar 1960.

On the Ergodic Theorem for Positive Linear Operators.

By *Eberhard Hopf*[1]) in Bloomington (Ind., U.S.A.).

Let X denote a space with points x and let there be given a σ-additive and σ-finite measure defined on all sets belonging to a given σ-field of subsets of X. All integrals $\int f$, $f = f(x)$, $x \in X$, are formed with this measure. If no domain of integration is indicated $\int f$ is extended through all of X. Denote by $L^1 = L^1(X)$ the linear space of all functions $f(x)$ integrable in X and consider a mapping $T = Tf$ of L^1 into L^1 which is linear and positive, $f \geqq 0$ (in X) $\rightarrow Tf \geqq 0$ (in X). A previous paper[2]) of the author dealt with those positive linear operators from L^1 to L^1 which conserve the integral, $\int Tf \equiv \int f$. They are closely connected with Markoff processes in X, and positivity and conservation of the integral arise simply from the requirement that a probability distribution in X goes over again into such a distribution. The author tried unsuccessfully to prove that the quotients $(n = 1, 2, \ldots)$

$$(1) \qquad Q_n(f, p) = \frac{S_n(f)}{S_n(p)}, \quad S_n(g) \equiv \sum_0^{n-1} T^i g,$$

converge almost everywhere in X if $f \in L^1$, $p \in L^1$, $p > 0$. In the mentioned paper this was proved under the additional hypothesis that the constants are in L^1 and that $T1 = 1$. For the corresponding Markoff process this hypothesis means that X has finite measure and that the measure is invariant under the process. In the special case where T is generated by a measure preserving point transformation $S = Sx$ of X into itself, $Tf(x) = f(Sx)$, this theorem coincides with G. D. Birkhoff's ergodic theorem. The general theorem had remained problematic for five years. In the case of point transformations, it covers the author's generalization of Birkhoff's theorem (infinite invariant measure) and the still more general theorem of W. Hurewicz (no invariant measure assumed) in the form given to it by P. Halmos, $Tf(x) = \omega(x) f(Sx)$ where $\omega(x) > 0$ is a suitably chosen fixed weight function.

Only quite recently R. V. Chacon and D. S. Ornstein succeeded in solving the problem. In their paper[3]) they prove the following somewhat more general

Ergodic theorem. *Let T be a positive linear operator from $L^1(X)$ to $L^1(X)$ with an L^1-norm $\leqq 1$. If $f \in L^1(X)$, $p \in L^1(X)$, $p \geqq 0$, then the quotients $Q_n(f, p)$, $n \rightarrow \infty$, have a finite limit in almost every point of the set where $\sum_0^\infty T^i p > 0$.*

It seemed desirable to us to present Chacon's and Ornstein's ingeneous proof in a more transparent form. This is what we do in the following lines. It is, in particular, the subsequent "Basic lemma 1" which seems to us to bring out more clearly the core

[1]) The author is indebted to the Office of Naval Research for a research grant at Indiana University.

[2]) *E. Hopf*, The general temporally discrete Markoff process. J. of Ratl. Mechanics and Analysis, **3** (1954), 13—45.

[3]) *R. V. Chacon* and *D. S. Ornstein*, A general ergodic theorem. Illinois J. of Mathematics, **4** (1960), 153—160.

of their reasoning. Our subsequent proof is very simple. Little touches have been applied in other places too to simplify the presentation. It must be said, however, that the principal ideas are those of Chacon and Ornstein.

The proof makes use of the lattice operations $f \to f^+$, $f \to f^-$ which carry L^1 into L^1,

$$f^+ = \max(f, 0), \; f^- = -\min(f, 0). \tag{2}$$

There holds

$$f = f^+ - f^-, \; |f| = f^+ + f^-. \tag{3}$$

f^+, f^- are both $\geqq 0$ but never both > 0. Therefore

$$f = f_2 - f_1, \; f_i \geqq 0 \quad \to \quad f^+ \leqq f_2, \; f^- \leqq f_1. \tag{4}$$

From $Tf = Tf^+ - Tf^-$, from the positivity of T and from (4) it follows that

$$(Tf)^+ \leqq Tf^+, \; (Tf)^- \leqq Tf^-, \; |Tf| \leqq T|f|. \tag{5}$$

The assumption that $|T| \leqq 1$ is equivalent to the statement that

$$\varphi \geqq 0 \to \int T\varphi \leqq \int \varphi. \tag{6}$$

The proof of the ergodic theorem is carried through in several steps the first of which is the proof of the

Basic lemma 1. *If $f \in L^1$ and if*

$$\sup_{n>0} \sum_0^{n-1} T^\nu f > 0$$

holds in each point of a set A (belonging to the given σ-field) then there exist, to each $\varepsilon > 0$, functions $h \in L^1$, $\varphi \in L^1$ such that

$\alpha)$ $h^- \leqq f^-$,
$\beta)$ $h = f + T\varphi - \varphi$, $\varphi \geqq 0$,
$\gamma)$ $\int h \leqq \int f$,
$\delta)$ $\int_A h^- < \varepsilon$.

Proof. We define a sequence of functions $h_i \in L^1$, $i \geqq 0$, $h_0 = f$, such that h_{i+1} is obtained from h_i on applying T only to its positive part,

$$h_{i+1} = Th_i^+ - h_i^-, \; h_0 = f. \tag{7}$$

We show that each $h = h_i$ has the properties $\alpha) - \gamma)$ and that $\delta)$ is satisfied for sufficiently large i. From (7), the positivity of T and from (4),

$$h_{i+1}^- \leqq h_i^- \tag{8}$$

and this implies $\alpha)$. (7) may be written

$$h_{i+1} = h_i + Th_i^+ - h_i^+.$$

Hence, by summation,

$$h_i = f + T\varphi_{i-1} - \varphi_{i-1}, \; \varphi_i = \sum_0^i h_\nu^+, \tag{9}$$

which proves $\beta)$. But $\beta)$ in turn implies $\gamma)$ by virtue of (6). From $\varphi_i - \varphi_{i-1} = h_i^+ \geqq h_i$ and from the first equation (9),

$$\varphi_i \geqq f + T\varphi_{i-1},$$

$i > 0$. As T is order-preserving this implies, by induction, that

$$\varphi_i \geqq \sum_0^{i-1} T^\nu f + T^i \varphi_0,$$

$i > 0$. As $\varphi_0 = h_0^+ = f^+ \geqq f$ it follows finally that

$$\varphi_i = \sum_0^i h_\nu^+ \geqq \sum_0^i T^\nu f,$$

$i > 0$. Evidently this holds for $i = 0$ too. This inequality and the hypothesis of the lemma imply now: In each point of A at least one of the h_ν^+, $\nu \geqq 0$, is positive or, in other words, at least one of the h_ν^- is zero. Hence, from (8), $h_n^- \geqq 0$, it follows that $h_n^- \downarrow 0$ in A and, consequently, that $\int_A h_n^- \to 0$. Lemma 1 is herewith completely proved.

Lemma 2. *If $f \in L^1$ and if*

$$\sup_{n>0} \sum_0^{n-1} T^\nu f \geqq 0$$

holds everywhere in a set A then f satisfies

$$\int_A f + \int_{\bar{A}} f^+ \geqq 0, \quad \bar{A} = X - A.$$

Proof. We prove the lemma first under the more restrictive hypothesis that sup > 0 in A. For any given $\varepsilon > 0$, lemma 1 may be applied. From the statements δ), α), γ) of this lemma it follows that

$$-\varepsilon - \int_{\bar{A}} f^- < -\int_A h^- - \int_{\bar{A}} h^- = -\int h^- \leqq \int h \leqq \int f.$$

This is only another form of the desired inequality, but with $-\varepsilon$ in place of 0 on the right. This inequality is thereby proved since ε was arbitrary.

In order to prove the lemma under the original hypothesis, sup $\geqq 0$ in A, we need merely use a function $p \in L^1$, $p > 0$, (such a p exists as the measure was supposed to be σ-finite) and apply the restricted lemma to $f + \eta p$, $\eta > 0$, in place of f. On letting $\eta \to 0$ we obtain the complete proof of lemma 2.

Remark. Lemma 2 is completely equivalent to the author's lemma (l. c. [2]), the maximal ergodic theorem):

$$\int_B f \geqq 0$$

if B is the set of all points where $\sup_{n>0} \sum_0^{n-1} T^\nu f \geqq 0$ (or the set of all points where this sup is > 0). The equivalence follows from three simple facts. Firstly, the hypothesis of lemma 2 says that $A < B$. Secondly, the left hand side of the final inequality of lemma 2 equals

$$\int_B f + \int_C f^- + \int_{\bar{B}} f^+ \geqq \int_B f$$

where $C = B - A$. Thirdly, in $\bar{B}$ there holds sup $\leqq 0$ and, in particular, $f \leqq 0$ or, in other words, $f^+ = 0$. This makes the equivalence obvious.

Lemma 3. *Let $f \in L^1$, $p \in L^1$, $p \geqq 0$. Then*

$$\sup_{n>0} |Q_n(f, p)| < \infty$$

holds almost everywhere in the set where $p > 0$.

Proof. As $|Q_n(f, p)| \leqq Q_n(|f|, p)$ it suffices to prove the lemma for the case that $f \geqq 0$, and without the absolute value sign. Let A denote the subset of the set $[p > 0]$ where $\sup Q_n(f, p) = \infty$. For any number $\omega > 0$, lemma 2 may be applied to $f - \omega p$ and A as

$$Q_n(f - \omega p, p) = Q_n(f, p) - \omega.$$

Therefore,

$$\int_A (f - \omega p) + \int_{\bar{A}} (f - \omega p)^+ \geqq 0.$$

From $f - \omega p \leqq f$, $f \geqq 0$ it follows that $(f - \omega p)^+ \leqq f$. Hence,

$$\int_A p \leqq \frac{1}{\omega} \int f.$$

As $p > 0$ in A and as ω is arbitrary A must have measure zero. Lemma 3 is thereby proved.

Lemma 4. *If $f \in L^1$, $p \in L^1$, $p \geqq 0$ then*

$$\lim_{n \to \infty} T^n f / \sum_0^{n-1} T^\nu p = 0$$

Proof. It suffices to prove this for the case $f \geqq 0$. Choose a number $\varepsilon > 0$ arbitrarily and consider the functions

$$g_n = T^n f - \varepsilon \sum_0^{n-1} T^\nu p, \quad g_0 = f$$

which satisfy the relations

$$g_{n+1} + \varepsilon p = T g_n. \tag{10}$$

It is sufficient to show, for almost every point of the set $[p > 0]$, that $g_n < 0$ for all large n or, in other words, that $\Sigma\, \chi_n$ converges where χ_n is the characteristic function of the set $[g_n \geqq 0]$. From $\chi_n g_n = g_n^+$ and (10),

$$\begin{aligned} \int g_{n+1}^+ + \varepsilon \int \chi_{n+1}\, p &= \int \chi_{n+1}\, (g_{n+1} + \varepsilon p) \\ &= \int \chi_{n+1}\, T g_n \leqq \int \chi_{n+1}\, T g_n^+ \leqq \int T g_n^+ \leqq \int g_n^+. \end{aligned}$$

By summation of the resulting inequalities from $n = 0$ on,

$$\int g_n^+ + \varepsilon \int p \sum_1^n \chi_\nu \leqq \int g_0^+$$

and, hence,

$$\int p \sum_1^\infty \chi_\nu \leqq \frac{1}{\varepsilon} \int g_0^+.$$

This obviously implies what we want to show and lemma 4 is herewith completely proved.

The next lemma contains the principal part of the proof of the ergodic theorem. Its proof is based upon lemma 1 but it makes use also of lemma 4.

Lemma 5. *Let $f \in L^1$, $p \in L^1$, $p \geqq 0$. If in each point of a set A there holds $p > 0$, $\sum_0^\infty T^\nu p = \infty$ and*

$$\underline{\lim}\, Q_n(f, p) < a < b < \overline{\lim}\, Q_n(f, p)$$

where a, b are numbers then A has measure zero.

Proof. Choose a number $\varepsilon > 0$. Part of the hypothesis says that in the set A

$$\sup_{n > 0} Q_n(f - bp) \geqq \overline{\lim}\, Q_n(f - bp) > 0.$$

Therefore we may apply lemma 1 to $f - bp$ in place of f. There exists a function $h \in L^1$ (the h of lemma 1 is now written in the form $h - bp$) such that α)

$$(h - bp)^- \leqq (f - bp)^- \tag{11}$$

and δ)

$$\int_A (h - bp)^- < \varepsilon. \tag{12}$$

(11) is equivalent to the statement that $h < bp$ implies $h \geqq f$. Consequently ($a < b$), $h < ap$ implies $h \geqq f$ which means that

$$(h - ap)^- \leqq (f - ap)^- \tag{13}$$

holds too. Now we make use of β) of lemma 1,

$$Q_n(h, p) = Q_n(f, p) + (T^n \varphi - \varphi) \Big/ \sum_0^{n-1} T^i p,$$

and we apply lemma 4 to φ, p. We also use the hypothesis that $\sum^{\infty} T^i p = \infty$ on A. It follows that $Q_n(h, p)$ has the same upper and the same lower limit as $Q_n(f, p)$ in each point of A (except in the points of a nulset which may be neglected in what follows). In particular,

$$\underline{\lim}\, Q_n(h, p) < a \quad \text{or} \quad \overline{\lim}\, Q_n(ap - h, p) > 0 \text{ in } A.$$

Consequently, lemma 1 may be applied to $ap - h$ in place of the f there. The new auxiliary function h of this lemma is now written in the form $ap - f'$. It follows from γ) that

$$\int (ap - f') \leqq \int (ap - h) \text{ or } \int (f' - ap) \geqq \int (h - ap), \tag{14}$$

and from α) that

$$(ap - f')^- \leqq (ap - h)^- \text{ or } (f' - ap)^+ \leqq (h - ap)^+, \tag{15}$$

and, finally, from δ) that

$$\int_A (ap - f')^- = \int_A (f' - ap)^+ < \varepsilon. \tag{16}$$

On using the first relation (3) we can write the inequality (14), second form,

$$\int (f' - ap)^- \leqq \int (h - ap)^- + \int [(f' - ap)^+ - (h - ap)^+]. \tag{17}$$

As the integrand in the last integral is $\leqq 0$ (see (15)) the inequality stays true if the integral is taken over A. Now,

$$(h - ap)^+ \geqq h - ap = h - bp + (b - a)\, p \geqq -(h - bp)^- + (b - a)\, p.$$

Consequently, the right hand side of (17) does not exceed

$$\int (h - ap)^- + \int_A (f' - ap)^+ + \int_A (h - bp)^- - (b - a) \int_A p.$$

We apply (13) to the first term, (16) to the second term and (12) to the third term. Thereby we obtain the inequality

$$\int (f' - ap)^- \leqq \int (f - ap)^- + 2\varepsilon - (b - a) \int_A p \tag{18}$$

in which h no longer appears. By the same reasoning as above it follows that $Q_n(f', p)$ has the same upper and the same lower limit as $Q_n(h, p)$ in each point of A. The final result is the following. If f satisfies the hypothesis of the present lemma then there exists, to any given $\varepsilon > 0$, a function f' which satisfies the same hypothesis and, in addition, the inequality (18). This result may in turn be applied to f': There exists a function f'' which satisfies the hypothesis of the present lemma and the inequality

$$\int (f'' - ap)^- \leqq \int (f' - ap)^- + 2\varepsilon - (b - a) \int_A p,$$

and so forth. On adding up the first n of these inequalities and on observing that the integral remaining on the left is $\geqq 0$ we find that

$$n[(b-a)\int_A p - 2\varepsilon] \leqq \int (f-ap)^-$$

holds for any integer n. Therefore, the number between the square brackets is $\leqq 0$. Since $\varepsilon > 0$ was arbitrary it follows that $\int_A p = 0$ and, since $p > 0$ was assumed in A, that A has measure zero. Lemma 5 is hereby proved.

Proof of the ergodic theorem. First we prove the theorem for the set where $p > 0$. It suffices to prove it for the case that $f \geqq 0$ (in X). Lemma 3 implies that the (finite or infinite) limit if it exists must be finite almost everywhere. So we need only prove existence. Within the part of the set $[p > 0]$ in which $\sum^{\infty} T^i p < \infty$ this is trivial because then $\overline{\lim}\, Q_n < \infty$ implies that the series $\sum^{\infty} T^i f$ with non-negative terms has a finite sum. In the remaining part $[p > 0,\ \sum T^i p = \infty]$ the positivity of the measure of the set where $\underline{\lim} < \overline{\lim}$ would imply the existence of numbers a, b, $a < b$, such that the set $[\underline{\lim} < a < b < \overline{\lim}]$ would have positive measure, in contradiction to lemma 5. Hence, $\underline{\lim} = \overline{\lim}$ holds almost everywhere in that remaining part.

In order to prove the theorem under the hypothesis mentioned there, i. e. for the set where $\sum^{\infty} T^i p > 0$, we observe that this set is the union of the sets $[p > 0]$ and

$$[S_{k+1}p > 0,\ S_k p = 0],\ k > 0. \tag{19}$$

In this set, $T^k p = S_{k+1}p - S_k p > 0$. On letting

$$f' = T^k f,\ p' = T^k p$$

we see that

$$Q_{n-k}(f', p') = \frac{S_n f - S_k f}{S_n p} = Q_n(f, p) - \frac{S_k f}{S_n p}$$

holds in this set and for $n > k$. From this formula and from what we have proved before it is evident that $\lim Q_n(f, p)$ exists and is finite almost everywhere in the set (19). The theorem is hereby completely proved.

Eingegangen 15. Januar 1960.

Über ein (max, min)-Theorem in der Theorie der Protoverbände und Dreigespanne.

Von *Fritz Klein-Barmen* in Wuppertal.

1. In zwei früheren Arbeiten[1]) habe ich im Rahmen der Theorie der abstrakten distributiven Verbände einen Satz bewiesen, aus dem durch Realisierung mehrere bemerkenswerte (max, min)-Identitäten und darauf zurückführbare (v, t)-Identitäten elementar arithmetischer und zahlentheoretischer Natur hervorgehen.

In der vorliegenden Untersuchung zeige ich durch Konstruktion des *Dreigespanns*, einer dem multiplikativen Verband[2]) ähnlichen Algebra mit drei binären Operationen, deren Kern ein noch näher zu beschreibender *Protoverband* ist, daß das in [10] angegebene Axiomensystem ohne Schaden für das genannte Theorem abgeschwächt, — anders ausgedrückt — daß der Gültigkeitsbereich des Theorems vergrößert, und zwar ganz beträchtlich vergrößert werden kann.

2. Es sei M eine abstrakte endliche oder unendliche Menge. Kleine lateinische Buchstaben sollen, wenn nichts anderes bestimmt wird, Elemente von M bezeichnen. Durch $\mathfrak{v}$, $\cup$, $\cap$ und $\circ$ seien binäre Operationen symbolisiert.

Zunächst einige Definitionen und Hilfssätze. M heißt ein *Operativ* in bezug auf $\mathfrak{v}$, wenn das Existentialaxiom[3])

$$\text{I.} \qquad \forall x \forall y \exists z \} \, x \mathfrak{v} y = z$$

in Kraft ist. Ist M ein Operativ in bezug auf $\mathfrak{v}$, so sei $x_1 \mathfrak{v} \cdots \mathfrak{v} x_m$ der durch

$$(1) \qquad x_1 \mathfrak{v} \cdots \mathfrak{v} x_{m+1} = (x_1 \mathfrak{v} \cdots \mathfrak{v} x_m) \, \mathfrak{v} \, x_{m+1} \qquad (m \geqq 2)$$

rekurrent erzeugte Term.

Die Verknüpfung $\mathfrak{v}$ heiße *assoziativ* bzw. *kommutativ* bzw. *autogen*[4]) in M, wenn M ein Operativ in bezug auf $\mathfrak{v}$ ist und II bzw. III bzw. IV gilt:

$$\text{II.} \qquad \forall x \forall y \forall z \} \, (x \mathfrak{v} y) \, \mathfrak{v} z = x \mathfrak{v} (y \mathfrak{v} z),$$

$$\text{III.} \qquad \forall x \forall y \} \, x \mathfrak{v} y = y \mathfrak{v} x,$$

$$\text{IV.} \qquad \forall x \forall y \forall z \} \, (x \mathfrak{v} y) \, \mathfrak{v} z = (x \mathfrak{v} z) \, \mathfrak{v} (y \mathfrak{v} z).$$

Wegen (1) können in II und IV die runden Klammern links vom Gleichheitszeichen fortgelassen werden. Durch Induktion ergibt sich:

Satz 1. *Ist $\mathfrak{v}$ autogen in M, so ist*

$$(2) \qquad (x_1 \mathfrak{v} \cdots \mathfrak{v} x_m) \, \mathfrak{v} z = (x_1 \mathfrak{v} z) \, \mathfrak{v} \cdots \mathfrak{v} (x_m \mathfrak{v} z) \qquad (m \geqq 2).$$

---

[1]) Vgl. [8], 320 u. [10], 90.

[2]) Näheres über multiplikative Verbände in [1], 200 u. [3], 127 sowie in [2] und [10].

[3]) Bei der Formulierung der Axiome wird von der logistischen Schreibweise Gebrauch gemacht; unter $\forall x\}$ ist der *Alloperator*, unter $\exists x\}$ der *Existenzoperator* zu verstehen.

[4]) Statt „autogen" werden auch die Bezeichnungen „unsymmetrisch-assoziativ" und „autodistributiv" verwendet; vgl. [4], [5] u. [11], 50.

Satz 2. *Ist* $\mathfrak{v}$ *autogen in* M *und* e *ein in bezug auf* $\mathfrak{v}$ *links neutrales Element von* M, *d. h. ist für alle Elemente* $e\mathfrak{v}x = x$, *so sind die Elemente von* M *idempotent in bezug auf* $\mathfrak{v}$.

Beweis. Für alle x ist

$$(e\mathfrak{v}e)\,\mathfrak{v}x = (e\mathfrak{v}x)\,\mathfrak{v}(e\mathfrak{v}x).$$

Satz 3. *Ist* $\mathfrak{v}$ *assoziativ und autogen in* M, *so ist für alle Elemente*

$$x\mathfrak{v}x\mathfrak{v}x = x\mathfrak{v}x\mathfrak{v}x\mathfrak{v}x.$$

Beweis. Für alle x ist

$$(x\mathfrak{v}x)\,\mathfrak{v}x = (x\mathfrak{v}x)\,\mathfrak{v}(x\mathfrak{v}x) = (x\mathfrak{v}x\mathfrak{v}x)\,\mathfrak{v}x,$$

woraus die Behauptung auf Grund der Festsetzung (1) folgt.

M heiße ein *distributiver Protoverband* in bezug auf $(\cup, \cap)$, wenn erstens M ein Operativ in bezug auf jede der beiden Verknüpfungen, zweitens $\cup$ autogen in M und drittens $\cup$ mit $\cap$ durch

V. $$\forall x \forall y \forall z\}\,(x \cap y) \cup z = (x \cup z) \cap (y \cup z)$$

gekoppelt ist [5]).

Analog zu Satz 1 gilt:

Satz 4. *Ist* M *ein distributiver Protoverband in bezug auf* $(\cup, \cap)$, *so ist*

(3) $$(x_1 \cap \cdots \cap x_m) \cup z = (x_1 \cup z) \cap \cdots \cap (x_m \cup z) \qquad (m \geqq 2).$$

Die Bezeichnung „distributiver Protoverband" ist durch den Umstand gerechtfertigt, daß es sich bei dieser Algebra um eine embryonale Entwicklungsstufe auf dem Weg zum distributiven Quasiverband [6]) handelt, der selbst wieder eine Etappe auf dem weiteren Weg zum gewöhnlichen distributiven Verband ist.

Satz 2 läßt sich folgendermaßen ausbauen:

Satz 5. *Ist* M *ein distributiver Protoverband in bezug auf* $(\cup, \cap)$, *ist* e *links neutral in bezug auf* $\cup$ *und gilt* $e \cap e = e$, *so sind die Elemente von* M *idempotent in bezug auf jede der beiden Verknüpfungen.*

Beweis. Wegen Satz 2 ist nur nachzuweisen, daß alle x idempotent in bezug auf $\cap$ sind. Das folgt aber sofort aus

$$(e \cap e) \cup x = (e \cup x) \cap (e \cup x).$$

M heiße ein *Dreigespann* in bezug auf $(\cup, \cap; \circ)$, wenn erstens M ein Operativ in bezug auf jede der drei Verknüpfungen, zweitens M ein distributiver Protoverband in bezug auf $(\cup, \cap)$, drittens $\circ$ assoziativ und kommutativ in M und viertens $\circ$ mit $\cup$ und $\cap$ durch

VI. $$\forall x \forall y\}\,(x \cup y) \circ (x \cap y) = x \circ y$$

gekoppelt ist.

Zur Illustrierung des Begriffs einige Beispiele.

Sind $\cup$ und $\cap$ die durch

$$\forall x \forall y\}\; x \cup y = x, \; \forall x \forall y\}\; x \cap y = y$$

definierten Verknüpfungen [7]), ist $\circ$ irgendeine in M assoziative und kommutative Verknüpfung, so ist M ein Dreigespann in bezug auf $(\cup, \cap; \circ)$.

---

[5]) In dem Fall, daß $\cup$ und $\cap$ dieselbe Verknüpfung symbolisieren, besagen IV und V dasselbe.

[6]) Die Theorie der Quasi-Verbände (Schief- oder Schrägverbände) ist — unabhängig voneinander — von P. Jordan in [6], [7] und S. Matsushita in [12], [13], [14] begründet worden.

[7]) Danach ist M ein *schiefer Halbverband* sowohl in bezug auf $\cup$ als auch in bezug auf $\cap$, wobei jedes Element rechts neutral in bezug auf $\cup$ und links neutral in bezug auf $\cap$ ist. Den Begriff des schiefen Halbverbandes habe ich in [9] eingeführt.

Ist $\cup$ die durch

$$\forall x \forall y \} \; x \cup y = c$$

definierte Verknüpfung, wobei c ein beliebiges, aber festes Element aus M ist, ist M überdies ein Operativ in bezug auf eine der Bedingung $c \cap c = c$ unterworfene Verknüpfung $\cap$, so ist M ein Dreigespann in bezug auf $(\cup, \cap; \cup)$.

Ist M ein gewöhnlicher Halbverband in bezug auf $\cup$, so ist M ein Dreigespann in bezug auf $(\cup, \cup; \cup)$.

3. Es sei M ein Dreigespann in bezug auf $(\cup, \cap; \circ)$. Ist m eine vorgegebene natürliche Zahl, so sei

$$(4) \qquad \lambda_1, \ldots, \lambda_\mu \qquad (1 \leqq \lambda_1 < \cdots < \lambda_\mu \leqq m; \; \mu = 1, \ldots, m)$$

eine der μ-gliedrigen Teilfolgen der Folge $1, \ldots, m$. Es seien $x_1, \ldots, x_m$ Elemente aus M, wobei für $\mu \neq \mu'$ sowohl $x_\mu = x_{\mu'}$ als auch $x_\mu \neq x_{\mu'}$ sein kann, was bei den Anwendungen zu beachten ist. Der Teilfolge (4) werde der $\cup$-Term $x_{\lambda_1} \cup \cdots \cup x_{\lambda_\mu}$ zugeordnet. Es sei

$$(5) \qquad \overset{m}{P}_{\lambda_1, \ldots, \lambda_\mu} (x_{\lambda_1} \cup \cdots \cup x_{\lambda_\mu})$$

das $\circ$-Produkt aller $\cup$-Terme, die bei festen Werten von m und μ den $\binom{m}{\mu}$ verschiedenen Teilfolgen (4) entsprechen. Ist kein Mißverständnis zu befürchten, so werde statt (5) einfach

$$\overset{m}{P}(x_{\lambda_1} \cup \cdots \cup x_{\lambda_\mu})$$

geschrieben. Insbesondere ist

$$\overset{m}{P}(x_{\lambda_1}) = x_1 \circ \cdots \circ x_m, \quad \overset{m}{P}(x_{\lambda_1} \cup \cdots \cup x_{\lambda_m}) = x_1 \cup \cdots \cup x_m.$$

Im Hinblick auf das (max, min)-Theorem ist es zweckmäßig, zwei Zählfunktionen einzuführen. Ist r eine reelle, hier übrigens stets natürliche Zahl, so sei $\gamma(r)$ die größte *gerade* Zahl, die nicht größer als r ist, und $\omega(r)$ die größte *ungerade* Zahl, die nicht größer als r ist. Die beiden Funktionen hängen vermöge der Gleichungen

$$\gamma(r+1) = \omega(r) + 1, \; \omega(r+1) = \gamma(r) + 1$$

zusammen.

Dies vorausgeschickt lautet das **(max, min)-Theorem:**

Für $m \geqq 2$ ist

$$(6) \qquad (x_1 \cap \cdots \cap x_m) \circ \overset{m}{P}(x_{\lambda_1} \cup x_{\lambda_2}) \circ \overset{m}{P}(x_{\lambda_1} \cup x_{\lambda_2} \cup x_{\lambda_3} \cup x_{\lambda_4}) \circ \cdots$$
$$= \overset{m}{P}(x_{\lambda_1}) \circ \overset{m}{P}(x_{\lambda_1} \cup x_{\lambda_2} \cup x_{\lambda_3}) \circ \cdots,$$

wobei die $\cup$-Terme vor dem Gleichheitszeichen aus einer geraden Zahl von Gliedern bestehen, die linke Seite der Gleichung (6) *also mit*

$$\overset{m}{P}(x_{\lambda_1} \cup \cdots \cup x_{\lambda_{\gamma(m)}})$$

abbricht, während die $\cup$-Terme nach dem Gleichheitszeichen aus einer ungeraden Zahl von Gliedern bestehen, die rechte Seite von (6) *also mit*

$$\overset{m}{P}(x_{\lambda_1} \cup \cdots \cup x_{\lambda_{\omega(m)}})$$

abbricht.

Für $m = 1$ artet (6) in die Trivialität $x_1 = x_1$ aus.

Wird

$$\breve{Q}_\mu(x_1, \ldots, x_m) = \overset{m}{P}(x_{\lambda_1} \cup \cdots \cup x_{\lambda_\mu}) \tag{7}$$

gesetzt, so läßt sich (6) kürzer so schreiben:

$$(x_1 \cap \cdots \cap x_m) \circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(x_1, \ldots, x_m) = \underset{\substack{\mu=1\\(u)}}{\overset{\omega(m)}{P}} \breve{Q}_\mu(x_1, \ldots, x_m). \tag{6*}$$

Dabei durchläuft μ links die geraden Zahlen von 2 bis $\gamma(m)$, rechts die ungeraden Zahlen von 1 bis $\omega(m)$.

Beweis. Die Behauptung ist für $m = 2$ nach VI richtig. Der Nachweis dafür, daß aus der Gültigkeit für irgendeinen Wert von m die Gültigkeit für $m + 1$ folgt, verläuft folgendermaßen. Nach (1) und VI ist

$$(x_1 \cap \cdots \cap x_{m+1}) \circ ((x_1 \cap \cdots \cap x_m) \cup x_{m+1}) = (x_1 \cap \cdots \cap x_m) \circ x_{m+1}.$$

Setzt man

$$x_\mu \cup x_{m+1} = y_\mu \quad (\mu = 1, \ldots, m), \tag{8}$$

so ist nach (3)

$$(x_1 \cap \cdots \cap x_{m+1}) \circ (y_1 \cap \cdots \cap y_m) = (x_1 \cap \cdots \cap x_m) \circ x_{m+1}.$$

Indem man beide Seiten der Gleichung mit

$$\underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(x_1, \ldots, x_m) \circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(y_1, \ldots, y_m)$$

durch $\circ$ verknüpft und berücksichtigt, daß $\circ$ assoziativ und kommutativ ist, erhält man

$$\begin{aligned}(x_1 \cap \cdots \cap x_{m+1}) &\circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(x_1, \ldots, x_m) \circ (y_1 \cap \cdots \cap y_m) \circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(y_1, \ldots, y_m)\\ &= (x_1 \cap \cdots \cap x_m) \circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(x_1, \ldots, x_m) \circ x_{m+1} \circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(y_1, \ldots, y_m)\end{aligned}$$

und daraus durch zweimalige Anwendung von (6*)

$$\begin{aligned}(x_1 \cap \cdots \cap x_{m+1}) &\circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(x_1, \ldots, x_m) \circ \underset{\substack{\mu=1\\(u)}}{\overset{\omega(m)}{P}} \breve{Q}_\mu(y_1, \ldots, y_m)\\ &= \underset{\substack{\mu=1\\(u)}}{\overset{\omega(m)}{P}} \breve{Q}_\mu(x_1, \ldots, x_m) \circ x_{m+1} \circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m)}{P}} \breve{Q}_\mu(y_1, \ldots, y_m).\end{aligned}$$

Die Hilfsgrößen $y_1, \ldots, y_m$ lassen sich vermittels der aus (8) gemäß (2) entspringenden Gleichungen

$$y_{\lambda_1} \cup \cdots \cup y_{\lambda_\mu} = x_{\lambda_1} \cup \cdots \cup x_{\lambda_\mu} \cup x_{m+1} \quad (\mu = 1, \ldots, m) \tag{9}$$

eliminieren. Faßt man für $\mu = 1, \ldots, m - 1$ die zu einem bestimmten μ gehörenden Terme

$$x_{\lambda_1} \cup \cdots \cup x_{\lambda_\mu} \cup x_{m+1} \quad (1 \leqq \lambda_1 < \cdots < \lambda_\mu \leqq m)$$

mit $\breve{Q}_{\mu+1}(x_1, \ldots, x_m)$ zu $\breve{Q}_{\mu+1}(x_1, \ldots, x_{m+1})$ zusammen und beachtet man, daß (9) für $\mu = m$ den Term $x_1 \cup \cdots \cup x_{m+1}$ liefert, so ergibt sich

$$(x_1 \cap \cdots \cap x_{m+1}) \circ \underset{\substack{\mu=2\\(g)}}{\overset{\gamma(m+1)}{P}} \breve{Q}_\mu(x_1, \ldots, x_{m+1}) = \underset{\substack{\mu=1\\(u)}}{\overset{\omega(m+1)}{P}} \breve{Q}_\mu(x_1, \ldots, x_{m+1}),$$

womit die Allgemeingültigkeit von (6*) bewiesen ist.

4. Es soll noch auf die zu Anfang erwähnten Realisierungen eingegangen werden. R sei die Menge der *reellen*, G^+ die Menge der *natürlichen* Zahlen. Mit $v(x, y)$ werde das *kleinste gemeinschaftliche Vielfache*, mit $t(x, y)$ der *größte gemeinschaftliche Teiler* der natürlichen Zahlen x und y bezeichnet. In Tab. 1 sind die Daten zusammengestellt, die den verschiedenen Realisierungen zugrunde liegen.

M	$x \cup y$	$x \cap y$	$x \circ y$
R	$\max(x, y)$	$\min(x, y)$	$x + y$
R	$\max(x, y)$	$\min(x, y)$	xy
G^+	$v(x, y)$	$t(x, y)$	xy

Tab. 1.

Man überzeugt sich leicht, daß für jede der drei Realisierungen die acht konstituierenden Axiome, nämlich

$$\mathrm{I}_\cup,\ \mathrm{I}_\cap,\ \mathrm{I}_\circ,\ \mathrm{II}_\circ,\ \mathrm{III}_\circ,\ \mathrm{IV}_\cup,\ \mathrm{V},\ \mathrm{VI}$$

in Kraft sind[8]). Das Kopplungsaxiom V geht bei den beiden ersten Realisierungen in

$$\max\big(\min(x, y), z\big) = \min\big(\max(x, z), \max(y, z)\big),$$

bei der dritten in

$$v\big(t(x, y), z\big) = t\big(v(x, z), v(y, z)\big),$$

das Kopplungsaxiom VI in die in Tab. 2 aufgeführten Identitäten über.

$(x \cup y) \circ (x \cap y) = x \circ y$
$\max(x, y) + \min(x, y) = x + y$
$\max(x, y) \min(x, y) = xy$
$v(x, y)\, t(x, y) = xy$

Tab. 2.

Gemäß (5) und (7) verwandelt sich $\breve{Q}_\mu(x_1, \ldots, x_m)$ bei den drei Realisierungen der Reihe nach in

$$\sum_{\lambda_1, \ldots, \lambda_\mu}^{m} \max(x_{\lambda_1}, \ldots, x_{\lambda_\mu}),\quad \prod_{\lambda_1, \ldots, \lambda_\mu}^{m} \max(x_{\lambda_1}, \ldots, x_{\lambda_\mu}),\quad \prod_{\lambda_1, \ldots, \lambda_\mu}^{m} v(x_{\lambda_1}, \ldots, x_{\lambda_\mu}).$$

Nach (4) ist dabei über alle Systeme $\lambda_1, \ldots, \lambda_\mu$ zu addieren bzw. zu multiplizieren, für die $1 \leqq \lambda_1 < \cdots < \lambda_\mu \leqq m$ ist. Wegen der Assoziativität und Kommutativität der max- wie auch der v-Verknüpfung kann diese Bestimmung durch die weitergehende ersetzt werden, daß über alle μ-gliedrigen Kombinationen ohne Wiederholung zu addieren bzw. zu multiplizieren ist, die sich vermittels der Zahlen $1, \ldots, m$ bilden lassen.

Die auf Grund der beschriebenen Realisierungen aus (6*) hervorgehenden Formeln sind:

$$\min(x_1, \ldots, x_m) + \sum_{\substack{\mu=2\\(g)}}^{\gamma(m)} \sum_{\lambda_1, \ldots, \lambda_\mu}^{m} \max(x_{\lambda_1}, \ldots, x_{\lambda_\mu}) = \sum_{\substack{\mu=1\\(u)}}^{\omega(m)} \sum_{\lambda_1, \ldots, \lambda_\mu}^{m} \max(x_{\lambda_1}, \ldots, x_{\lambda_\mu}), \tag{10. 1}$$

$$\min(x_1, \ldots, x_m) \prod_{\substack{\mu=2\\(g)}}^{\gamma(m)} \prod_{\lambda_1, \ldots, \lambda_\mu}^{m} \max(x_{\lambda_1}, \ldots, x_{\lambda_\mu}) = \prod_{\substack{\mu=1\\(u)}}^{\omega(m)} \prod_{\lambda_1, \ldots, \lambda_\mu}^{m} \max(x_{\lambda_1}, \ldots, x_{\lambda_\mu}), \tag{10. 2}$$

$$t(x_1, \ldots, x_m) \prod_{\substack{\mu=2\\(g)}}^{\gamma(m)} \prod_{\lambda_1, \ldots, \lambda_\mu}^{m} v(x_{\lambda_1}, \ldots, x_{\lambda_\mu}) = \prod_{\substack{\mu=1\\(u)}}^{\omega(m)} \prod_{\lambda_1, \ldots, \lambda_\mu}^{m} v(x_{\lambda_1}, \ldots, x_{\lambda_\mu}). \tag{10. 3}$$

[8]) Der untere Index zeigt an, auf welche der Verknüpfungen sich das betreffende Axiom bezieht.

Hinzuzufügen ist, daß es zu jeder Realisierung ein duales Gegenstück gibt. Man erhält dasselbe, indem man in allen Termen max und min bzw. v und t miteinander vertauscht.

Prinzipiell anders hat D. S. Mitrinovitch die Identitäten (10. 1), (10. 2), (10. 3) hergeleitet. Er folgert dieselben nicht wie hier aus einem übergeordneten formalen Theorem, sondern beweist sie direkt, ohne die konkrete Zahlenebene zu verlassen[9]).

Eine Folgerung mag noch erwähnt werden. Sind $x_1, \ldots, x_m$ natürliche Zahlen mit

$$\min(x_1, \ldots, x_m) = 1 \text{ bzw. } t(x_1, \ldots, x_m) = 1,$$

so kann in (10. 2) bzw. (10. 3) der erste Faktor links vom Gleichheitszeichen unterdrückt werden, während sich rechts für das zu $\mu = 1$ gehörende Produkt beidemal $x_1 \cdots x_m$ ergibt. Sind $x_1, \ldots, x_m$ insbesondere die ganzen Zahlen von 1 bis m und wird $x_\nu = \nu$ gesetzt, so ist für $m \geqq 3$ nach (10. 2)

$$m! = \frac{\prod\limits_{\substack{\mu=2 \\ (g)}}^{\gamma(m)} \prod\limits_{\lambda_1,\ldots,\lambda_\mu}^{m} \max(\lambda_1, \ldots, \lambda_\mu)}{\prod\limits_{\substack{\mu=3 \\ (u)}}^{\omega(m)} \prod\limits_{\lambda_1,\ldots,\lambda_\mu}^{m} \max(\lambda_1, \ldots, \lambda_\mu)}.$$

und nach (10. 3)

$$m! = \frac{\prod\limits_{\substack{\mu=2 \\ (g)}}^{\gamma(m)} \prod\limits_{\lambda_1,\ldots,\lambda_\mu}^{m} v(\lambda_1, \ldots, \lambda_\mu)}{\prod\limits_{\substack{\mu=3 \\ (u)}}^{\omega(m)} \prod\limits_{\lambda_1,\ldots,\lambda_\mu}^{m} v(\lambda_1, \ldots, \lambda_\mu)}.$$

---

[9]) Vgl. [15]. Unter der engeren Voraussetzung, daß $x_1, \ldots, x_m$ nichtnegative ganze Zahlen sind, findet sich (10. 1) bereits in [16], 121 u. 329.

Literaturverzeichnis.

[1] *G. Birkhoff*, Lattice theory. New York 1948.

[2] *A. C. Choudhury*, The doubly distributive m-lattice. Bull. Calcutta math. Soc. **49** (1957), 71—74.

[3] *M. L. Dubreil-Jacotin, L. Lesieur* u. *R. Croisot*, Leçons sur la théorie des treillis. Paris 1953.

[4] *W. Felscher*, Ein unsymmetrisches Assoziativ-Gesetz in der Verbandstheorie. Arch. Math. **8** (1957), 171—174.

[5] *W. Felscher* u. *F. Klein-Barmen*, Zur Axiomatik der kommutativen Halbverbände. Arch. Math. **10** (1959), 7.

[6] *P. Jordan* u. *E. Witt*, Zur Theorie der Schrägverbände. Abh. Akad. Wiss. u. Lit. Mainz 1953, 225—232.

[7] *P. Jordan* u. *W. Böge*, Zur Theorie der Schrägverbände. II. Abh. Akad. Wiss. u. Lit. Mainz 1954, 79—92.

[8] *F. Klein-Barmen*, Zur Theorie der abstrakten Verknüpfungen. Math. Ann. **105** (1931), 308—323.

[9] *F. Klein-Barmen*, Über eine weitere Verallgemeinerung des Verbandsbegriffes. Math. Z. **46** (1940), 472—480.

[10] *F. Klein-Barmen*, Über Verbände mit einer weiteren assoziativen und kommutativen Elementverknüpfung. Math. Z. **47** (1940), 85—104.

[11] *F. Klein-Barmen*, Verallgemeinerung des Verbandsbegriffs durch Abschwächung des Axioms der Idempotenz. Math. Z. **70** (1958), 38—51.

[12] *S. Matsushita*, Lattices non commutatifs. C. R. Acad. Sci. Paris 1953, 1526—1527.

[13] *S. Matsushita*, Ideals in Non-commutative Lattices. Proc. Jap. Acad. **34** (1958), 407—410.

[14] *S. Matsushita*, Zur Theorie der nichtkommutativen Verbände. I. Math. Ann. **137** (1959), 1—8.

[15] *D. S. Mitrinovitch*, Sur certaines relations restant valables si l'on permute les opérateurs y intervenant. Bull. Soc. math. phys. R. P. Serbie 8 (1956), 15—21.

[16] *G. Pólya* u. *G. Szegö*, Aufgaben und Lehrsätze aus der Analysis. II. Berlin 1925.

Eingegangen 11. Februar 1960.

Bemerkungen zu einem Satz von Pontrjagin und Tschebotarjow.

Von *Johannes Thomas* in Potsdam.

1. Fragestellung.

Im Anschluß an eine Abhandlung von L. S. Pontrjagin ([1], S. 116) bewiesen N. G. Tschebotarjow und N. N. Meiman ([2], S. 255) folgenden

Satz (*). *In dem „Quasipolynom"*

$$F(\lambda) = \sum_{l=0}^{t} \sum_{k=1}^{k(l)} a_{lk} \lambda^l e^{h_{lk}\lambda} \tag{1}$$

$$(t \geqq 1,\ k(l) \geqq 0\,^{1)},\ k(t) \geqq 1,\ a_{lk} \neq 0,\ h_{lk} \text{ reell},\ h_{lk} < h_{l,k+1})$$

sei mindestens ein zu einem Index $l \leqq t-1$ gehörendes Summenglied vorhanden, und es sei mindestens einer der Werte $h_{l,k(l)}$ $(l = 0, \ldots, t-1)$ größer als $h_{t,k(t)}$. Dann besitzt $F(\lambda)$ eine unendliche Menge von Nullstellen λ_m $(m = 1, 2, 3, \ldots)$ derart, daß die mit einer gewissen positiven Konstanten p und einer gewissen Teilfolge $\{M_m\}$ der Folge der natürlichen Zahlen gebildete Folge

$$\lambda_m - (p \ln M_m + i M_m) \tag{2}$$

konvergent ist $(i = \sqrt{-1})$.

Die Konstante p ist folgendermaßen definiert: Wird der Wert $\operatorname{Max}_{l=0,\ldots,t-1} h_{l,k(l)}$ für die Indizes $l = l^{(\nu)}$ angenommen, so ist

$$p = \operatorname*{Max}_{l > \operatorname{Max}_\nu l^{(\nu)}} \frac{l - \operatorname{Max}_\nu l^{(\nu)}}{h_{l^{(\nu)},k(l^{(\nu)})} - h_{l,k(l)}}\ ^{2)}. \tag{2a}$$

Ist $k(t) = 1$, so kann man mit Heranziehung des Stieltjesschen Integralbegriffs auch

$$F(\lambda) = (-1)^t a_{t1} e^{h_{t1}\lambda} \operatorname{Det}\left(\int_{-N}^{N} e^{-\lambda s} dr_{ij}(s) - \lambda \delta_{ij}\right)_{i,j=1,\ldots,t} \tag{3}$$

schreiben, wo δ_{ij} das Kroneckersymbol, N eine positive Zahl, die größer als $\operatorname{Max} |h_{lk} - h_{t1}|$ ist,

$$r_{ij}(s) = \tfrac{1}{2}\delta_{i,j-1}(1 + \operatorname{sgn} s) \quad (i = 1, \ldots, t-1) \tag{3a}$$

und $r_{ij}(s)$ eine (komplexwertige) Treppenfunktion ist, deren Sprungrelationen

$$r_{ij}(h_{t1} - h_{j-1,k} - 0) - r_{ij}(h_{t1} - h_{j-1,k} + 0) = \frac{a_{j-1,k}}{a_{t1}} \quad (k = 1, \ldots, k(j-1)) \tag{3b}$$

---

[1]) $k(l) = 0$ bedeutet, daß in der Summe kein Glied mit der betreffenden Potenz λ^l als Faktor auftritt.

[2]) Die Positivwertigkeit von p ergibt sich so: Für $l = t > \operatorname{Max}_\nu l^{(\nu)}$ gilt nach Voraussetzung $h_{t,k(t)} < h_{l^{(\nu)},k(l^{(\nu)})}$, woraus $p \geqq \dfrac{t - \operatorname{Max}_\nu l^{(\nu)}}{h_{l^{(\nu)},k(l^{(\nu)})} - h_{t,k(t)}} > 0$ folgt.

lauten; die Aufgabe der Ermittlung von Nullstellen der Funktion $F(\lambda)$ ist dann die Aufgabe der Nullstellenermittlung bei der in (3) stehenden Determinante als Funktion von λ.

Die Theorie der Systeme linearer Integrodifferentialgleichungen veranlaßte nun A. D. Myschkis, die Frage aufzuwerfen, ob sich über eine Determinante der in (3) stehenden Gestalt eine der Aussage des obigen Satzes (*) entsprechende Aussage auch dann machen läßt, wenn man von den Funktionen $r_{ij}(s)$ lediglich voraussetzt, daß sie von beschränkter Schwankung sind ([3], S. 27). Mit dieser Frage wollen wir uns nachstehend befassen.

2. Generelle Voraussetzungen, Vorbemerkung.

Es sei

$$D(\lambda) = \operatorname{Det}\left(\int_{-N}^{N} e^{-\lambda s} dr_{ij}(s) - \lambda\delta_{ij}\right)_{i,j=1,\ldots,n} \qquad (N > 0,\ n \geqq 1) \tag{4}$$

die zu betrachtende Determinante[3]). *Wir fassen ausschließlich Werte λ ins Auge, deren Realteile nichtnegativ sind.* Die in (4) vorkommenden n^2 *Funktionen* $r_{ij}(s)$ sehen wir als *komplexwertig* an; von ihnen setzen wir, wie gesagt, generell voraus, *daß sie in dem Intervall* $-N \leqq s \leqq N$ *von beschränkter Schwankung sind.* Wir nehmen

$$r_{ij}(-N) = 0 \qquad (i, j = 1, \ldots, n) \tag{5}$$

an und erweitern, um im folgenden einige Formeln bequemer schreiben zu können, den Definitionsbereich der $r_{ij}(s)$ auf alle reellen Zahlen, indem wir

$$\begin{cases} r_{ij}(s) \equiv 0 & \text{für } s < -N \\ r_{ij}(s) \equiv r_{ij}(N) & \text{für } s > N \end{cases} \tag{6}$$

setzen. Bezeichnen wir die obere Grenze der Zahlen $s \leqq N$, für welche $\int_{-N}^{s} |r_{ij}(\sigma)|\, d\sigma$ verschwindet, mit b_{ij}, so ist

$$\int_{-N}^{N} e^{-\lambda s} dr_{ij}(s) = e^{-\lambda b_{ij}} R_{ij}(\lambda) \tag{7}$$

mit

$$\begin{aligned} R_{ij}(\lambda) &= \int_{b_{ij}-0}^{N} e^{-\lambda(s-b_{ij})}\, dr_{ij}(s) \\ &= r_{ij}(N)\, e^{-\lambda(N-b_{ij})} + \lambda \int_{b_{ij}+0}^{N} e^{-\lambda(s-b_{ij})}\, r_{ij}(s)\, ds \qquad (b_{ij} \leqq N). \end{aligned} \tag{8}$$

Bei einem Wert λ mit positivem Realteil können wir

$$R_{ij}(\lambda) = \lambda \int_{0}^{\infty} e^{-\lambda x} r_{ij}(b_{ij} + x)\, dx \tag{9}$$

schreiben ([4], S. 71).

3. Zwei Sätze über die Nullstellen von $D(\lambda)$ mit nichtnegativen Realteilen.

Nachstehend beweisen wir jetzt zwei Sätze, die von Nullstellen mit nichtnegativen Realteilen der Funktion $D(\lambda)$ handeln. Der zweite dieser Sätze ist ein Existenzsatz für solche Nullstellen und stellt eine Verallgemeinerung des in Absatz 1 formulierten Satzes (*) in dem genannten Sinn dar.

Satz 1. *Bei der in* (4) *stehenden Funktion $D(\lambda)$ ist für das Vorhandensein unendlich vieler Nullstellen mit nichtnegativen Realteilen notwendig, daß mindestens eine der Zahlen b_{ij} negativ ist.*

[3]) Bis auf das erste Integral auf der rechten Seite der Gleichung (29), welches im Lebesgueschen Sinn zu verstehen ist, sind alle Integrale im Riemann-Stieltjesschen bzw. Riemannschen Sinn gemeint.

Beweis. Wir zeigen, daß dann, wenn alle $b_{ij} \geqq 0$ sind, die Anzahl der Nullstellen von $D(\lambda)$, die einen nichtnegativen Realteil haben, beschränkt ist.

Setzt man (7) in (4) ein und entwickelt man die in (4) stehende Determinante, so erhält man einen Ausdruck

$$D(\lambda) = (-1)^n \lambda^n \left(1 + \sum_{l=1}^{n} \sum_{k=1}^{k(l)} A_{lk}(\lambda)\, \lambda^{-l} e^{H_{lk}\lambda}\right), \tag{10}$$

in dem die $k(l) \geqq 0$, die $H_{lk} \geqq 0$ und die $A_{lk}(\lambda)$ algebraische Summen aus Produkten der $R_{ij}(\lambda)$ sind. Aus (8) ist ersichtlich, daß die $R_{ij}(\lambda)$ beschränkt bleiben, wenn λ mit einem nichtnegativen Realteil gegen ∞ strebt ([4], S. 479). Das hat zur Folge, daß der Ausdruck, den die in (10) stehende runde Klammer enthält, für alle λ-Werte von Null verschieden ist, deren Realteil nichtnegativ ist und deren Betrag eine gewisse positive Zahl überschreitet. Dieser Tatbestand liefert aber in Verbindung mit der Holomorphie von $D(\lambda)$ alsdann die zu beweisende Beschränktheit der Anzahl der Nullstellen von $D(\lambda)$ mit nichtnegativen Realteilen. Damit ist Satz 1 bewiesen.

Für den nunmehr zu formulierenden Satz 2 fügen wir in bezug auf die Funktionen $r_{ij}(s)$ den in Absatz 2 gemachten Annahmen noch folgende hinzu:

Es existieren Ableitungsordnungen $m_{ij} \geqq 0$ folgender Art: Bei noch näher zu kennzeichnenden $\varepsilon_{ij} > 0$ sind die Funktionen $r_{ij}(s)$ in den Intervallen $b_{ij} < s < b_{ij} + \varepsilon_{ij}$ mindestens m_{ij}-mal differenzierbar; die Funktionen $r_{ij}^{(m_{ij})}(s)$ haben in diesen Intervallen eine Ableitung im Lebesgueschen Sinne ([4], S. 103), *und für die (dann vorhandenen) einseitigen Grenzwerte $r_{ij}^{(\mu)}(b_{ij} + 0)$ $(\mu = 0, \ldots, m_{ij})$ gelten die Gleichungen*

$$r_{ij}^{(\mu)}(b_{ij} + 0) = 0 \quad (\mu = 0, \ldots, m_{ij} - 1); \quad r_{ij}^{(m_{ij})}(b_{ij} + 0) = c_{ij} \neq 0\ ^{4)}. \tag{11}$$

Unter den von uns gemachten zusätzlichen Voraussetzungen über die $r_{ij}(s)$ ordnen wir der Funktion $D(\lambda)$ in (4) die Funktion

$$D_1(\lambda;\, z_{ij}) = \lambda^P \operatorname{Det}\left(z_{ij}\, \lambda^{-m_{ij}} e^{-\lambda b_{ij}} - \lambda \delta_{ij}\right)_{i,j=1,\ldots,n} \tag{12}$$

zu, wobei die z_{ij} komplexe Parameter sind und P eine nichtnegative ganze Zahl derart ist, daß $D_1(\lambda;\, z_{ij})$ nach Entwicklung der in (12) stehenden Determinante in ein Quasipolynom der Gestalt

$$D_1(\lambda;\, z_{ij}) = \sum_{l=0}^{t} \sum_{k=1}^{k(l)} a_{lk}(z_{ij})\, \lambda^l e^{h_{lk}\lambda} \tag{1'}$$

$$(t = n + P \geqq 1,\ k(t) = 1,\ a_{t1} = (-1)^n,\ h_{t1} = 0;\ k(l) \geqq 0,\ h_{lk} \text{ reell},\ h_{lk} < h_{l,k+1})$$

übergeht. Die $a_{lk}(z_{ij})$ sind algebraische Summen aus Produkten der z_{ij} und damit stetige Funktionen des Systems aller z_{ij}. Mit Beachtung von (7) liefert ein Vergleich von (4) und (12) sofort die Gleichung

$$D(\lambda) = \lambda^{-P} D_1(\lambda;\, \lambda^{m_{ij}} R_{ij}(\lambda)). \tag{13}$$

Erfüllt das Quasipolynom (1′) die Voraussetzungen des Satzes (∗), so können wir uns der beim Satz (∗) eingeführten Nomenklatur bedienen und im Anschluß an (2a) die Größe

$$q = \operatorname*{Max}_{\nu}\ l^{(\nu)} + p h_{l^{(\nu)},k(l^{(\nu)})} \tag{14}$$

---

[4]) Zur Existenz dieser Grenzwerte siehe [4], S. 100.

einführen. Diejenigen Indizes l, für welche die Gleichung

$$l + p h_{l,k(l)} = q \tag{15}$$

besteht, bezeichnen wir mit l_σ $(\sigma = 1, \ldots, s)$. Man hat $s \geqq 2$ [5]).

Satz 2. *Die gemäß* (12) *definierte Funktion* $D_1(\lambda; z_{ij})$ *erfülle, in der Gestalt* (1′) *geschrieben, die Voraussetzungen des Satzes* $(*)$, *und von den* s *Zahlen* $a_{l_\sigma, k(l_\sigma)}(c_{ij})$ *seien wenigstens zwei von Null verschieden; für die Größen* ε_{ij} *gelte*

$$\varepsilon_{ij} > \frac{m_{ij}}{p}. \tag{16}$$

Dann besitzt die in (4) *stehende Funktion* $D(\lambda)$ *eine unendliche Menge von Nullstellen* λ_m $(m = 1, 2, 3, \ldots)$ *derart, daß die mit einer gewissen Teilfolge* $\{M_m\}$ *der Folge der natürlichen Zahlen gebildete Folge*

$$\lambda_m - (p \ln M_m + i M_m) \tag{17}$$

konvergent ist.

Beweis. Den Beweis des Satzes 2 führen wir nach dem Vorbild des Beweises von Satz $(*)$ in [2], wobei wir ebenso wie beim Beweis des Satzes 1 die Theorie der Laplacetransformation hinzuziehen.

Wir wählen aus der Folge der natürlichen Zahlen eine Teilfolge $\{\widetilde{M}_\mu\}$ $(\mu = 1, 2, 3, \ldots)$ so aus, daß alle s Folgen $\left\{e^{i\frac{q-l_\sigma}{p}\widetilde{M}_\mu}\right\}$ $(\sigma = 1, \ldots, s)$ konvergieren, und schreiben

$$\lim_{\mu \to \infty} e^{i\frac{q-l_\sigma}{p}\widetilde{M}_\mu} = a_\sigma \qquad (|a_\sigma| = 1). \tag{18}$$

Da voraussetzungsgemäß mindestens zwei der Größen $a_{l_\sigma, k(l_\sigma)}(c_{ij})$ von Null verschieden sind, hat die in bezug auf $\vartheta^{-\frac{1}{p}}$ algebraische Gleichung

$$\sum_{\sigma=1}^{s} a_{l_\sigma, k(l_\sigma)}(c_{ij})\, a_\sigma i^{l_\sigma} \left(\vartheta^{-\frac{1}{p}}\right)^{l_\sigma} = 0 \tag{19}$$

mindestens eine von Null verschiedene Wurzel ϑ. Setzen wir mit einer solchen Wurzel ϑ

$$\lambda = \lambda_\mu(\zeta) = p \ln \widetilde{M}_\mu + i\widetilde{M}_\mu + \ln \vartheta + \zeta \qquad (-\pi < \operatorname{Im}(\ln \vartheta) \leqq \pi) \tag{20}$$

und schreiben wir

$$D_1(\lambda_\mu(\zeta); z_{ij}) = \widetilde{M}_\mu^{\,q} \left(\sum_{\sigma=1}^{s} a_{l_\sigma, k(l_\sigma)}(z_{ij})\, a_\sigma i^{l_\sigma} \vartheta^{\frac{q-l_\sigma}{p}} e^{\frac{q-l_\sigma}{p}\zeta} + u_\mu(\zeta; z_{ij}) \right), \tag{21}$$

so ist $u_\mu(\zeta; z_{ij})$ offenbar eine bezüglich ζ holomorphe und bezüglich des Systems der z_{ij} stetige Funktion. In jedem beschränkten komplexen $(\zeta; z_{ij})$-Bereich gilt gleichmäßig

$$\lim_{\mu \to \infty} u_\mu(\zeta; z_{ij}) = 0 \quad ([2], \text{S. } 256). \tag{22}$$

---

[5]) Es kann $l_1 = \operatorname{Max}_\nu l^{(\nu)}$ gesetzt werden; dann ist $l_2, \ldots, l_s$ die Menge der Indizes $l > \operatorname{Max}_\nu l^{(\nu)}$, für welche der Quotient $\dfrac{l - \operatorname{Max}_\nu l^{(\nu)}}{h_{l^{(\nu)}, k(l^{(\nu)})} - h_{l, k(l)}}$ den maximalen Wert p annimmt.

Unter Beachtung von (13) und (21) bilden wir die Funktion

$$
\begin{aligned}
(23)\qquad v_\mu(\zeta) &= \widetilde{M}_\mu^{-q}\left[\lambda_\mu(\zeta)^p D(\lambda_\mu(\zeta)) - D_1(\lambda_\mu(\zeta); c_{ij})\right] \\
&= \widetilde{M}_\mu^{-q}\left[D_1\big(\lambda_\mu(\zeta);\ \lambda_\mu(\zeta)^{m_{ij}} R_{ij}(\lambda_\mu(\zeta))\big) - D_1(\lambda_\mu(\zeta);\ c_{ij})\right] \\
&= \sum_{\sigma=1}^{s}\left[a_{l_\sigma, k(l_\sigma)}\big(\lambda_\mu(\zeta)^{m_{ij}} R_{ij}(\lambda_\mu(\zeta))\big) - a_{l_\sigma, k(l_\sigma)}(c_{ij})\right] a_\sigma i^{l_\sigma} \vartheta^{\frac{q-l_\sigma}{p}} e^{\frac{q-l_\sigma}{p}\zeta} \\
&\quad + u_\mu\big(\zeta;\ \lambda_\mu(\zeta)^{m_{ij}} R_{ij}(\lambda_\mu(\zeta))\big) - u_\mu(\zeta;\ c_{ij}).
\end{aligned}
$$

Es ist $v_\mu(\zeta)$ eine holomorphe Funktion von ζ, und nach dem eben Gesagten ist klar, daß in jedem beschränkten Bereich der komplexen ζ-Ebene gleichmäßig

$$(24)\qquad \lim_{\mu\to\infty} v_\mu(\zeta) = 0$$

gelten wird, falls in jedem solchen ζ-Bereich gleichmäßig die Limesrelationen

$$(25)\qquad \lim_{\mu\to\infty} \lambda_\mu(\zeta)^{m_{ij}} R_{ij}(\lambda_\mu(\zeta)) = c_{ij}$$

bestehen. Wir beweisen (25) nachher und knüpfen an (24) an. Schreiben wir gemäß (23) und (21)

$$(26)\qquad D(\lambda_\mu(\zeta)) = \lambda_\mu(\zeta)^{-p}\widetilde{M}_\mu^q\left[\vartheta^{\frac{q}{p}} e^{\frac{q}{p}\zeta}\sum_{\sigma=1}^{s} a_{l_\sigma, k(l_\sigma)}(c_{ij})\, a_\sigma i^{l_\sigma}\vartheta^{-\frac{l_\sigma}{p}} e^{-\frac{l_\sigma}{p}\zeta} + u_\mu(\zeta; c_{ij}) + v_\mu(\zeta)\right],$$

so ist bei Beachtung der Holomorphie von $u_\mu(\zeta; c_{ij})$ und $v_\mu(\zeta)$ sowie der Gleichungen (19), (22) und (24) folgendes ersichtlich: Umgeben wir den Nullpunkt der komplexen ζ-Ebene mit einer Kreiskontur $\mathfrak{K}_r$ von (beliebig kleinem) Radius r derart, daß die in (26) in der eckigen Klammer stehende, von μ unabhängige σ-Summe auf $\mathfrak{K}_r$ von Null verschieden ist, so gibt es eine natürliche Zahl $\mu(r)$ derart, daß für alle $\mu \geqq \mu(r)$ die Funktionen $D(\lambda_\mu(\zeta))$ innerhalb $\mathfrak{K}_r$ mindestens eine Nullstelle haben. Wir lassen die Radiuslängen r eine eigentlich monotone Nullfolge $\{r_m\}$ $(m = 1, 2, 3, \ldots;\ r_1 \leqq \frac{1}{2})$ durchlaufen, konstruieren die Folge $\{\mu(r_m)\}$ als eigentlich monoton steigende Folge und setzen

$$(27)\qquad \widetilde{M}_{\mu(r_m)} = M_m\ ^{6)}.$$

Ist dann $\zeta = \zeta_m$ eine Nullstelle von $D(\lambda_{\mu(r_m)}(\zeta))$ innerhalb $\mathfrak{K}_{r_m}$, so ist

$$(28)\qquad \lambda_m = p\ \ln M_m + iM_m + \ln\vartheta + \zeta_m$$

eine Nullstellenfolge der Funktion $D(\lambda)$, für welche die Folge (17) konvergiert.

Es fehlt noch der Beweis von (25): Gehen wir bei $R_{ij}(\lambda)$ von der Schreibweise (9) aus und beachten wir (11), so erhalten wir

$$
\begin{aligned}
\lambda^{m_{ij}} R_{ij}(\lambda) - c_{ij} &= \int_0^{\varepsilon_{ij}} e^{-\lambda x} r_{ij}^{(m_{ij}+1)}(b_{ij} + x)\, dx \\
(29)\qquad &\quad + \lambda^{m_{ij}} e^{-\lambda\varepsilon_{ij}}\left[\lambda\int_0^\infty e^{-\lambda t} r_{ij}(b_{ij} + \varepsilon_{ij} + t)\, dt - \sum_{\mu=0}^{m_{ij}} \lambda^{\mu - m_{ij}} r_{ij}^{(m_{ij}-\mu)}(b_{ij} + \varepsilon_{ij})\right].
\end{aligned}
$$

Durchläuft λ die Folge (20), wobei ζ einem beschränkten Bereich der komplexen ζ-Ebene angehören mag, so strebt auf der rechten Seite von (29) das erste Integral gleichmäßig in ζ gegen Null ([4], S. 171), und das Integral in der eckigen Klammer bleibt beschränkt ([4], S. 480). Des weiteren erhalten wir mit Beachtung von (16) bei Durchlaufung der Folge (20) gleichmäßig in ζ den Sachverhalt

$$(30)\qquad \lambda^{m_{ij}} e^{-\lambda\varepsilon_{ij}} = e^{-\varepsilon_{ij}(i\widetilde{M}_\mu + \ln\vartheta + \zeta)}\left(p\frac{\ln\widetilde{M}_\mu}{\widetilde{M}_\mu} + \frac{\ln\vartheta + \zeta}{\widetilde{M}_\mu} + i\right)^{m_{ij}} \cdot \widetilde{M}_\mu^{m_{ij} - p\varepsilon_{ij}} \to 0 \text{ für } \mu\to\infty.$$

---

6) Die Forderung $r_1 \leqq \frac{1}{2}$ gewährleistet, daß in der komplexen λ-Ebene die den Kreiskonturen $\mathfrak{K}_{r_m}$ der ζ-Ebene entsprechenden Kreiskonturen $|\lambda - (p\ln M_m + iM_m + \ln\vartheta)| = r_m$ disjunkt liegen.

Die Beachtung der Beschränktheit auch der μ-Summe in (29) liefert schließlich dann die Limesrelationen (25) gleichmäßig in jedem beschränkten ζ-Bereich.

Damit ist Satz 2 bewiesen.

Sind im besonderen die n^2 Funktionen $r_{ij}(s)$ sämtlich reellwertig, so erhalten wir den konjugiert komplexen Wert von $D(\lambda)$, indem wir dort λ durch den konjugiert komplexen Wert $\bar{\lambda}$ ersetzen. Es hat dies zur Folge, daß zugleich mit den Werten λ_m, von denen Satz 2 spricht, auch deren konjugiert komplexe Werte $\bar{\lambda}_m$ Nullstellen von $D(\lambda)$ sind.

Literatur.

[1] *L. S. Pontrjagin*, Über die Nullstellen einiger elementarer transzendenter Funktionen (russisch). Nachr. d. Akad. d. Wiss. d. UdSSR, Math. Serie 6: **3** (1942), 115—134.

[2] *N. G. Tschebotarjow* und *N. N. Meiman*, Das Routh-Hurwitzsche Problem für Polynome und ganze Funktionen (russisch). Trudy mat. Inst. Steklow, **26** (1949).

[3] *A. D. Myschkis*, Lineare Differentialgleichungen mit nacheilendem Argument, Berlin 1955.

[4] *G. Doetsch*, Handbuch der Laplace-Transformation, I, Basel 1950.

Eingegangen 17. Juni 1959.

Modulare Korrespondenzen und L-Reihen *).

Von *S. S. Rangachari* in Bombay.

Inhalt.

Einleitung.
Teil I. § 1. Der Körper der Modulfunktionen N-ter Stufe.
§ 2. Modulare Korrespondenzen.
§ 3. Darstellungen von modularen Korrespondenzen.
Teil II. § 4. Reduktionstheorie.
§ 5. Artinsche L-Reihen.
Teil III. § 6. Globale Artinsche L-Reihen.
Teil IV. § 7. Allgemeine Struktur globaler Artinscher L-Reihen.
Teil V. § 8. Einige Beispiele.
Anhang. Berechnung der Vielfachheit einer irreduziblen Darstellung.
Literatur.

Einleitung.

Die Theorie der „Hecke-Operatoren T_n" wurde von Hecke in zwei Arbeiten ([5], I, II) entwickelt und dann zum Studium der Arithmetik von Modulformen und Theta-Reihen verwendet. Seitdem wurden sie von verschiedenen Mathematikern im Zusammenhang mit zahlentheoretischen Problemen häufig untersucht. Ein neuer Zugang zum Studium dieser Operatoren wurde in der Arbeit von Eichler [4] eröffnet. Er hat diese Operatoren für Spitzenformen vom Grad — 2 zu einer gewissen Untergruppe der Modulgruppe als Differentiale gewisser Korrespondenzen abgeleitet, wobei diese Korrespondenzen einem geeigneten Körper von Modulfunktionen zugehören. Auf diese Weise gelang es ihm, die Hassesche Vermutung für diesen Körper zu beweisen.

Diese Methode von Eichler wurde von Shimura bei seinen Untersuchungen ([9], [10]) über Modularkorrespondenzen übernommen. Shimura nimmt die Hauptkongruenzuntergruppe $\Gamma_1(N)$ der Modulgruppe $\Gamma(1)$ und ordnet dieser Gruppe einen gewissen Funktionenkörper K über dem rationalen Zahlkörper Q zu. Er folgert aus gewissen Kongruenzrelationen und den Resultaten von Hecke über die Operatoren T_n die Richtigkeit der Hasseschen Vermutung für K.

In dieser Arbeit wird der Versuch unternommen, den Funktionenkörper K_N über $Q(\zeta_N)$ etwas näher zu analysieren ($K_N = K(\zeta_N)$, ζ_N ist eine primitive N-te Einheitswurzel). Wir betrachten K_N als Galois-Erweiterung des rationalen Funktionenkörpers

*) Diese Arbeit wurde im Jahre 1959 von der Mathematisch-Naturwissenschaftlichen Fakultät der Universität Göttingen als Dissertation angenommen (D 7). Herrn Prof. Dr. Deuring bin ich für mannigfache Anregungen und Ratschläge zu Dank verpflichtet.

mit der Galoisgruppe $\Gamma(1)/\Gamma_1(N)$ und verbinden mit jedem Charakter χ dieser Gruppe eine globale Artinsche L-Reihe, die analog zur Hasseschen Zetafunktion von K_N definiert ist.

Wenn die Stufe N eine ungerade Primzahl q ($\geqq 7$) ist, dann sind diese L-Reihen für gewisse Charaktere χ meromorphe Funktionen von s. Der Beweis gründet sich auf weiteren Korrespondenzrelationen zwischen den Modularkorrespondenzen und den Korrespondenzen, die den Elementen der endlichen Gruppe $\Gamma(1)/\Gamma_1(q)$ zugeordnet sind. Außerdem werden einige Resultate von Hecke über irreduzible Darstellungen von $\Gamma(1)/\Gamma_1(q)$ benutzt. Im letzten Teil werden einige weitere Nebenresultate über globale Artinsche L-Reihen im allgemeinen und einige Beispiele für die Stufe q im besonderen diskutiert.

In Teil I werden die notwendigen Vorbemerkungen über Modulfunktionenkörper und das Spezialisationsprinzip von Shimura gemacht. Wir definieren die Modularkorrespondenzen nach Shimura und beweisen einige Beziehungen zwischen diesen Korrespondenzen. Die Darstellungen dieser Korrespondenzen, die durch die Differentiale erster Gattung vermittelt werden, werden nach der Methode von Hecke studiert.

In Teil II wird unter Benutzung der Reduktionstheorie von Deuring und Shimura die Fortsetzung der Funktionalprimdivisoren auf eine Erweiterung des Konstantenkörpers betrachtet. Dann werden die Artinschen L-Reihen des reduzierten Funktionenkörpers eingeführt; wegen der Korrespondenzrelationen im reduzierten Körper erhält man für die L-Reihen explizite Ausdrücke.

Wir definieren die globale Artinsche L-Reihe in Teil III und beschränken uns in diesem ganzen Abschnitt auf Primzahlstufe $q \geqq 7$. Für gewisse Charaktere χ wird dann bewiesen, daß die globale Artinsche L-Reihe eine meromorphe Funktion von s ist, es wird sogar ein expliziter Ausdruck für diese abgeleitet.

In Teil IV wird die allgemeine Struktur globaler Artinscher L-Reihen studiert. Hier wird nach einem Verfahren von Taniyama ([11]) ein Kriterium für die Darstellbarkeit dieser Reihen als Produkte Heckescher L-Reihen hergeleitet, das sind L-Reihen mit Größencharakteren.

Schließlich geben wir einige Beispiele für Stufe q und gewisse Charaktere χ der endlichen Gruppe $\Gamma(1)/\Gamma_1(q)$, für welche die entsprechende globale Artinsche L-Reihe sich als ein Produkt von Heckeschen L-Reihen in $Q(\zeta_q)$ darstellen läßt.

Bezeichnungen.

Q: rationaler Zahlkörper;

C: komplexer Zahlkörper;

Z: der Ring der ganzen Zahlen;

$\Gamma(1)$: die Modulgruppe (die Gruppe aller Matrizen $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit ganzen Zahlen a, b, c, d und $ad - bc = 1$).

$\Gamma_1(N)$: die Hauptkongruenzuntergruppe mod N von $\Gamma(1)$, d. h. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ mit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N}$, wobei N eine natürliche Zahl ist;

$\Gamma_0(N)$: die Gruppe aller $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$ mit $c \equiv 0 \pmod{N}$.

$G_N^* = GL\,(2, Z/NZ)$: die Gruppe aller nicht singulären (2, 2)-Matrizen mit Restklassen modulo N als Elementen.

$S_N^* = SL\,(2, Z/NZ)$: die Untergruppe aller Matrizen aus G_N^* mit der Determinante 1.

Wenn k ein Körper ist, so soll $\bar{k}$ die algebraisch abgeschlossene Hülle von k bedeuten.

Teil I.

§ 1. Der Körper der Modulfunktionen N-ter Stufe.

Seien ω_1, ω_2 zwei komplexe Zahlen mit $\operatorname{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$ und bezeichnen wir mit D das durch (ω_1, ω_2) auf der komplexen Ebene $\boldsymbol{C}$ erzeugte Gitter. Wir setzen

$$\begin{aligned} g_2(D) &= g_2(\omega_1, \omega_2) = 60\, \Sigma' \omega^{-4}, \\ g_3(D) &= g_3(\omega_1, \omega_2) = 140\, \Sigma' \omega^{-6}, \\ \Delta(D) &= \Delta(\omega_1, \omega_2) = g_2^3(D) - 27 g_3^2(D), \\ \wp(z, D) &= \wp(z;\, \omega_1, \omega_2) = z^{-2} + \Sigma' [(z-\omega)^{-2} - \omega^{-2}], \end{aligned}$$

wo die Summation in Σ' über alle $\omega \in D$ $(\omega \neq (0, 0))$ läuft. Die Funktion $\wp$ und deren Ableitung $\wp'$ erfüllen die Gleichung

$$\wp'^2 = 4\wp^3 - g_2 \wp - g_3.$$

$g_2(\omega_1, \omega_2)$ und $g_3(\omega_1, \omega_2)$ sind Modulformen von der Stufe 1 und von Grad -4 bzw. -6. Mit $\tau = \frac{\omega_1}{\omega_2}$ bilden wir für jede natürliche Zahl N

$$(1) \qquad f_{\alpha\beta}(\tau) = f(\alpha, \beta;\, \tau) = \frac{g_2(\omega_1, \omega_2)}{g_3(\omega_1, \omega_2)}\, \wp\left(\frac{\alpha\omega_1 + \beta\omega_2}{N};\, \omega_1, \omega_2\right).$$

Die Funktionen $f_{\alpha\beta}(\tau)$ sind Modulfunktionen von der Stufe N. Man sieht leicht, daß $f_{\alpha\beta} = f_{\alpha'\beta'}$ dann und nur dann gilt, wenn $(\alpha, \beta) \equiv (\alpha', \beta')$ (mod N) ist.

Seien a, b, c, d ganze rationale Zahlen mit $ad - bc = 1$. Es gilt

$$(2) \qquad f\left(\alpha, \beta; \frac{a\tau + b}{c\tau + d}\right) = f(\alpha', \beta';\, \tau) \text{ für } (\alpha'\beta') \equiv (\alpha\,\beta)\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bmod N.$$

Wir bezeichnen mit $\mathfrak{M}_N$ den Körper aller Modulfunktionen der Stufe N. $\mathfrak{M}_N$ ist ein algebraischer Funktionenkörper. Ferner ist er eine Galoissche Erweiterung von $\mathfrak{M}_1 = \boldsymbol{C}(j(\tau))$ $\left(j(\tau) = \frac{g_2^3(\tau)}{\Delta(\tau)}\right)$, und die Galoisgruppe ist isomorph mit $S_N = S_N^*/\pm I$ derart, daß für jedes $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S_N^*$ die Abbildung $f(\tau) \to f\left(\frac{a\tau + b}{c\tau + d}\right)$ einen Autormorphismus von $\mathfrak{M}_N/\mathfrak{M}_1$ liefert.

Sei $\mathfrak{K}_N = Q(j(\tau), f_{\alpha\beta}(\tau))$ $(0 \leqq \alpha, \beta \leqq N-1,\ (\alpha, \beta) \neq (0, 0))$. Für eine Modulsubstitution $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ gilt $f\left(\frac{a\tau + b}{c\tau + d}\right) = f(\tau)$ für alle $f \in \mathfrak{K}_N$ genau dann, wenn $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \pm I$ (mod N) ist, wie man aus (1) und (2) sieht. Infolgedessen entsteht $\mathfrak{M}_N$ aus $\mathfrak{K}_N$ durch Konstantenerweiterung von Q zu $\boldsymbol{C}$. Mit anderen Worten:

$$(3) \qquad \mathfrak{M}_N = \boldsymbol{C}(j(\tau), f_{\alpha\beta}(\tau)).$$

Sei τ_0 eine derartige komplexe Zahl mit $\operatorname{Im} \tau_0 > 0$, daß $j(\tau_0)$ transzendent über Q ist. Setzen wir $j_0 = j(\tau_0)$, $\gamma_0 = \frac{27 j_0}{j_0 - 1}$ und sei E diejenige elliptische Kurve, die durch die Gleichung

$$Y^2 = 4X^3 - \gamma_0 X - \gamma_0$$

definiert ist. Wir wählen zwei komplexe Zahlen ω_{01}, ω_{02} derart, daß $\tau_0 = \frac{\omega_{01}}{\omega_{02}}$ ist, und es sei D_0 das Gitter, das durch $(\omega_{01}, \omega_{02})$ in C erzeugt wird. Dann gibt es stets einen analytischen Isomorphismus $u(z)$ von C/D_0 auf E. Nach Shimura ([10], S. 19) gilt

$$h(u(z)) = \frac{g_2(\omega_{01}, \omega_{02})}{g_3(\omega_{01}, \omega_{02})} \cdot \wp(z; \omega_{01}, \omega_{02}), \tag{4}$$

wo h die kanonische Funktion auf E ist.

Die Punkte von E bilden eine additive abelsche Gruppe. Setzen wir

$$g(N, E) = \{t \in E;\ Nt = 0\}$$

mit einer natürlichen Zahl N, dann ist $g(N, E)$ eine endliche abelsche Gruppe der Ordnung N^2 mit zwei Erzeugenden (t_1, t_2). Wir können $t_1 = u\left(\frac{\omega_{01}}{N}\right)$, $t_2 = u\left(\frac{\omega_{02}}{N}\right)$ wählen. Aus (4) sehen wir

$$j(E) = j(\tau_0),$$

$$h(\alpha t_1 + \beta t_2) = f_{\alpha\beta}(\tau_0) \quad (0 \leqq \alpha, \beta < N). \tag{5}$$

Wir bezeichnen mit $K_N^*(E)$ und $K_N(E)$ die Körper $Q(j_0, t)$ und $Q(j_0, h(t))$ (t läuft dabei über alle Punkte von $g(N, E)$). Beide sind Galoiserweiterungen von $Q(j_0)$; die Galoisgruppe von $K_N(E)/Q(j_0)$ sei $G_N(E)$. Jedes $\sigma \in G_N(E)$ läßt sich zu einem Automorphismus von $K_N^*(E)$ erweitern, indem man t_1^σ, t_2^σ so definiert, daß $h(t_1)^\sigma = h(t_1^\sigma)$ und $h(t_2)^\sigma = h(t_2^\sigma)$ gilt. (t_1^σ, t_2^σ) ist dann ein Erzeugendensystem von $g(N, E)$, so daß $\begin{pmatrix} t_1^\sigma \\ t_2^\sigma \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} t_1 \\ t_2 \end{pmatrix}$ mit einer Modulmatrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ist. Folglich gilt

$$h(\alpha t_1 + \beta t_2)^\sigma = h(\alpha' t_1 + \beta' t_2) \text{ mit } (\alpha'\ \beta') = (\alpha\ \beta) \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{6}$$

Dieser Automorphismus σ ist durch die Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ bestimmt und wird der der Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ bezüglich (t_1, t_2) zugeordnete Automorphismus von $K_N(E)$ genannt.

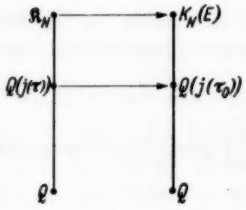


Fig. 1

Wegen (5) können wir (6) folgendermaßen umschreiben:

$$f_{\alpha\beta}(\tau_0)^\sigma = f_{\alpha'\beta'}(\tau_0) \text{ mit } (\alpha'\ \beta') = (\alpha\ \beta) \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{7}$$

Nach dem „Spezialisierungsprinzip" von Shimura ([10], S. 21) gibt es einen Isomorphismus zwischen $\mathfrak{K}_N$ und $K_N(E)$, für den $\tau \to \tau_0$, $j(\tau) \to j(\tau_0)$ gilt. Unter diesem Isomorphismus ist $f_{\alpha\beta}(\tau) \to f_{\alpha\beta}(\tau_0)$ und die Gleichung (7) wird jetzt

$$f_{\alpha\beta}(\tau)^\sigma = f_{\alpha'\beta'}(\tau) \text{ mit } (\alpha'\ \beta') = (\alpha\ \beta) \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{8}$$

Das bedeutet dann, daß wir für jeden Automorphismus σ von $\mathfrak{K}_N$ über $Q(j(\tau))$ eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_N^*$ haben. Diese Abbildung $\sigma \to \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ist dann ein Isomorphismus der Galoisgruppe von $\mathfrak{K}_N$ über $Q(j(\tau))$ auf G_N. (Prop. 5 in [10]). Wir bezeichnen daher die Galoissche Gruppe mit $G_N(E)$. Sei dann $S_N(E)$, das Urbild von S_N unter diesem Isomorphismus. $S_N(E)$ hängt nicht von (t_1, t_2) ab.

Wir übernehmen jetzt die folgenden Sätze von Shimura (Prop. 6 und 7 in [10]):

Satz 1. *Der Unterkörper von $K_N(E)$, der der Untergruppe $S_N(E)$ zugeordnet ist, ist nichts anderes als $Q(j_0, \zeta_N)$, wo ζ_N eine primitive N-te Einheitswurzel ist. $Q(\zeta_N)$ ist dann algebraisch abgeschlossen in $K_N(E)$.*

Satz 2. *Sei* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G_N^*$ *und* σ *der entsprechende Automorphismus von* $K_N(E)$. *Man hat dann* $\zeta_N^\sigma = \zeta_N^{ad-bc}$; *insbesondere ergibt, wenn* $ad - bc \equiv p \pmod N$ *ist* (p *eine Primzahl*), $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *den Frobeniusschen Automorphismus* $\sigma = \left(\frac{Q(\zeta_N)/Q}{p}\right)$ *in* $Q(\zeta_N)$.

Jetzt behaupten wir die Existenz eines Unterkörpers L von $K_N(E)$ mit der Eigenschaft $L > Q(j_0)$ und $L \cap Q(\zeta_N) = Q$. Ein solcher Körper kann folgendermaßen konstruiert werden ([10]):

Nach der Identifizierung der Gruppe $G_N(E)$ mit G_N durch den obigen Isomorphismus bezeichnen wir mit H_N die Untergruppe $\left(\begin{pmatrix} a & 0 \\ 0 & \pm 1 \end{pmatrix}, (a, N) = 1\right) \Big/ \pm I$ von G_N und mit L_N den entsprechenden Unterkörper. Dann haben wir

$$G_N = H_N S_N, \text{ mit } H_N \cap S_N = (1) \text{ und } L_N \cap Q(\zeta_N) = Q.$$

Ferner ist $L_N(\zeta_N) = K_N(E)$. L_N ist nun der gesuchte Körper L. Q ist algebraisch abgeschlossen in L_N.

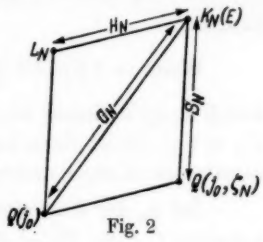


Fig. 2

Da Q in L algebraisch abgeschlossen ist, gibt es eine vollständige singularitätenfreie Kurve Γ, definiert bezüglich Q derart, daß $L = Q(u)$ mit einem allgemeinen Punkt u von Γ bezüglich Q ist. Wir bezeichnen die Kurve Γ in dem Fall, daß L_N statt L als Definitionskörper gewählt wird, mit Γ_N.

§ 2. Modulare Korrespondenzen.

Sei n eine positive ganze Zahl mit $(n, N) = 1$ und seien $g_\alpha (1 \leqq \alpha \leqq s)$ die sämtlichen zyklischen Untergruppen der Ordnung n von E. Nach einem Satz von Weil ([14], Prop. 10) gibt es elliptische Kurven E_α und Homomorphismen $\lambda_\alpha : E \to E_\alpha$ mit der Eigenschaft: Kern $\lambda_\alpha = g_\alpha$.

Wir bezeichnen mit j_α die birationale Invariante von E_α; die j_α sind alle algebraisch über $Q(j_0)$ und transzendent über Q. Es gibt für jedes α dann einen Isomorphismus $\tau_\alpha : Q(j_0) \to Q(j_\alpha)$ mit $j_0^{\tau_\alpha} = j_\alpha$.

Wenn $h_\alpha = h^{\tau_\alpha} (1 \leqq \alpha \leqq s)$ die kanonischen Funktionen von E_α sind, so gelten die folgenden zwei Sätze von Shimura (Prop. 9 und 10 in [10]).

Satz 3. *Es gibt für jedes* α *einen Isomorphismus* σ_α *von* $K_N(E)$ *auf* $K_N(E_\alpha)$ *mit* $j_0^{\sigma_\alpha} = j_\alpha$ *und* $h(t)^{\sigma_\alpha} = h_\alpha(\lambda_\alpha t)$ *für* $t \in g(N, E)$. *Der Isomorphismus* σ_α *ist durch diese Bedingungen eindeutig fixiert, weil* j_0 *und* $h(t)$ *den Körper* $K_N(E)$ *erzeugen.*

Satz 4. *Sei* $v = (v_1, \ldots, v_m)$ *eine endliche Menge von Elementen aus* $K_N(E)$ *mit* $j_0 \in Q(v)$. *Seien* $\sigma_\alpha (1 \leqq \alpha \leqq s)$ *die Isomorphismen von* $K_N(E)$ *aus Satz* 3. *Dann enthält* $Q(v, j^{\sigma_\alpha})$ *den Körper* $Q(v^{\sigma_\alpha})$ *und* $(v^{\sigma_1}, \ldots, v^{\sigma_s})$ *bildet ein vollständiges System bezüglich* $Q(v)$ *Konjugierter.*

Wir bezeichnen mit X_n den bezüglich Q *rationalen primen Divisor* auf der Produktmannigfaltigkeit $\Gamma \times \Gamma$ mit dem allgemeinen Punkt $u \times u^{\sigma_1}$ *bezüglich* Q. Nach Shimura nennen wir X_n eine *Modularkorrespondenz vom Grad* n *auf* Γ. Dann folgt aus Satz 4 und den Sätzen von Weil ([12], Th. 12, S. 204)

$$X_n \cdot (u \times \Gamma) = u \times \sum_{\alpha=1}^{s} u^{\sigma_\alpha} \text{ oder}$$

$$X_n(u) = \sum_{\alpha=1}^{s} u^{\sigma_\alpha}. \tag{9}$$

Es entspreche $\varrho_n \in G_n(E)$ der Matrix $\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \in G_N^*$ unter dem Isomorphismus zwischen $G_N(E)$ und G_N. Wir bezeichnen mit Y_n den Ort *von* $u \times u^{\varrho_n}$ *bezüglich* Q *auf* $\Gamma \times \Gamma$. Da ϱ_n zum Zentrum von $G_N(E)$ gehört, d. h.

$$\lambda \varrho_n(L) = \varrho_n \lambda(L) \text{ für jedes } \lambda \in G(K_N(E)/L)$$

gilt, so ist ϱ_n ein Automorphismus von L, d. h. $Q(u) = Q(u^{\varrho_n})$; daher ist Y_n eine birationale Korrespondenz von Γ und es gilt

$$Y_n(u) = u^{\varrho_n}. \tag{10}$$

(Es soll hier bemerkt werden, daß X_n, Y_n nur von der Restklasse von n modulo N abhängen.)

Wenn $\varphi \in S_N(E)$ das Urbild von $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S_N^*$ unter dem Isomorphismus ist, der durch $(t_1\, t_2)$ definiert ist, bezeichnen wir mit C den Ort von $u \times u^\varphi$ bezüglich $Q(\zeta_N)$ auf $\Gamma_N \times \Gamma_N$. Es ist dann klar, daß $K_N(E) = Q(\zeta_N, u) = Q(\zeta_N, u^\varphi)$ ist, oder: C definiert eine birationale Korrespondenz von Γ_N über $Q(\zeta_N)$. Ferner gilt $C(u) = u^\varphi$.

Sei φ_n der Automorphismus von $Q(\zeta_N)/Q$, für den φ_n: $\zeta_N \to \zeta_N^n$ gilt. Da jede Korrespondenz C über $Q(\zeta_N)$ definiert ist, hat sie eine Konjugierte C^{φ_n} unter diesem Isomorphismus; C^{φ_n} hat den allgemeinen Punkt $(u \times u^\varphi)^{\varphi_n}$, wo $u \times u^\varphi$ ein allgemeiner Punkt von C bezüglich $Q(\zeta_N)$ ist.

Die Beziehung zwischen C und C^{φ_n} wird durch den folgenden Satz erläutert.

Satz 5. *Wenn* $\tau_n \in G_N(E)$ *der Matrix* $\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \in G_N^*$ *zugeordnet ist, dann ist* C^{φ_n} *die Korrespondenz, die* $\tau_n^{-1} \cdot \varphi\tau_n \in S_N(E)$ *zugeordnet ist.*

Beweis. Sei $\tau_n' \in G_N(E)$ das Element zu $\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} \in G_N^*$. Dann folgt aus Satz 2, daß $\tau_n = \tau_n' = \varphi_n$ auf $Q(\zeta_N)$ ist. Ferner gilt $\tau_n \tau_n' = \varrho_n$, und da $\tau_n' \in H_N$ ist, $u^{\tau_n'} = u$. Jetzt folgt

$$\begin{aligned} (u \times u^\varphi)^{\varphi_n} &= (u \times u^\varphi)^{\tau_n} \\ &= u^{\tau_n} \times u^{\varphi\tau_n} \\ &= u^{\tau_n'\tau_n} \times u^{\tau_n \cdot \tau_n^{-1}\varphi\tau_n} \\ &= u^{\varrho_n} \times (u^{\tau_n'\tau_n})^{\tau_n^{-1}\varphi\tau_n} \\ &= u^{\varrho_n} \times (u^{\varrho_n})^{\tau_n^{-1}\varphi\tau_n}. \end{aligned} \tag{11}$$

$(u \times u^\varphi)^{\varphi_n}$ ist ein allgemeiner Punkt von C^{φ_n} bezüglich $Q(\zeta_N)$, so daß $u^{\varrho_n} \times (u^{\varrho_n})^{\tau_n^{-1}\varphi\tau_n}$ auch ein allgemeiner Punkt von C^{φ_n} bezüglich $Q(\zeta_N)$ ist, oder: C^{φ_n} ist die Korrespondenz, die $\tau_n^{-1}\varphi\tau_n$ zugeordnet ist, denn u^{ϱ_n} ist ein allgemeiner Punkt von Γ_N in bezug auf Q.

Wegen Satz 5 können wir behaupten, daß jeder Automorphismus von $Q(\zeta_N)/Q$ einen Automorphismus der Korrespondenzgruppe (C) induziert die den Elementen von $S_N(E)$ zugeordnet ist:

$$\varphi_n\colon\ \varphi \to \tau_n^{-1}\varphi\tau_n.$$

Da $\tau_n^{-1}\varphi\tau_n = \tau_n'\varphi\tau_n'^{-1}$ ist, so wird der Automorphismus φ_n durch φ_n: $\varphi \to \tau_n'\varphi\tau_n'^{-1}$ gegeben.

Bedeutet $\psi \in S_N(E)$ das Element, das $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in S_N^*$ zugeordnet ist, und bezeichnen wir die ψ entsprechende Korrespondenz mit A, dann gilt nach Shimura ([10], S. 11) folgender Satz:

Satz 6. *Es ist* $A^{\varphi_n} \cdot Y_n = A$ ($\cdot$ *bedeutet das Korrespondenzprodukt*).

Wir nennen zwei Matrizen $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ mit ganzzahligen Koeffizienten und der Determinante n *äquivalent*, wenn eine modulare Matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ mit der Eigenschaft $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ existiert. Man kann dann zeigen, daß es genau s Äquivalenzklassen solcher Matrizen gibt und die Repräsentanten $\begin{pmatrix} a_\nu & b_\nu \\ c_\nu & d_\nu \end{pmatrix}$ können sogar so gewählt werden, daß $\begin{pmatrix} a_\nu & b_\nu \\ c_\nu & d_\nu \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \pmod{N}$ gilt (Hecke [5], I).

Nach der Methode von Shimura gibt es einen Isomorphismus $\bar{\sigma}_\nu$ von $\mathfrak{K}_N$, definiert durch

$$g^{\bar{\sigma}_\nu}(\tau) = g^{\tau_n'}\left(\frac{a_\nu \tau + b_\nu}{c_\nu \tau + d_\nu}\right) \text{ für jedes } g \in \mathfrak{K}_N. \tag{12}$$

Man hat dann

$$j^{\bar{\sigma}_\nu}(\tau_0) = j(E_\nu)$$

und

$$f_{\alpha\beta}^{\bar{\sigma}_\nu}(\tau_0) = h_\nu(\lambda_\nu(\alpha t_1 + \beta t_2)). \tag{13}$$

Nach dem „Spezialisierungsprinzip" von Shimura können $(K_N, \sigma_\nu, K_N^{\sigma_\nu})$ und $(\mathfrak{K}_N, \bar{\sigma}_\nu, \mathfrak{K}_N^{\bar{\sigma}_\nu})$ identifiziert werden.

Sei $\mathfrak{L}_N$ der Unterkörper von $\mathfrak{K}_N$, der der Untergruppe H_N von G_N entspricht. Man kann $\mathfrak{L}_N$ als den Körper der rationalen Funktionen auf Γ_N bezüglich Q betrachten. Da $\tau_n' \in H_N$ ist, hat man aus (12):

$$g^{\bar{\sigma}_\nu}(\tau) = g\left(\frac{a_\nu \tau + b_\nu}{c_\nu \tau + d_\nu}\right) (1 \leqq \nu \leqq s) \text{ für jedes } g \in \mathfrak{L}_N. \tag{14}$$

Unter dem Isomorphismus zwischen $\mathfrak{K}_N$ und $K_N(E)$ geht $\mathfrak{L}_N$ in L_N über, und aus (14) folgt

$$g^{\sigma_\nu}(\tau_0) = g\left(\frac{a_\nu \tau_0 + b_\nu}{c_\nu \tau_0 + d_\nu}\right) (1 \leqq \nu \leqq s) \text{ für jedes } g \in L_N. \tag{15}$$

Für einen Automorphismus $\varphi \in G_N(E)$, der einer Modulsubstitution $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ entspricht, haben wir nach (7)

$$g^{\varphi}(\tau_0) = g\left(\frac{a\tau_0 + b}{c\tau_0 + d}\right) = g(\varphi(\tau_0)) \text{ für } g \in L_N.$$

Dann gilt nach (15)

$$g^{\varphi\sigma_\nu}(\tau_0) = (g^{\varphi}(\tau_0))^{\sigma_\nu} = g(\sigma_\nu(\varphi(\tau_0))).$$

Nun entspricht $\sigma_\nu \varphi$ der Substitution $\begin{pmatrix} a_\nu & b_\nu \\ c_\nu & d_\nu \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Da diese Matrix eine ganzzahlige Matrix mit der Determinante n ist, existiert ein Repräsentant $\begin{pmatrix} a_\mu & b_\mu \\ c_\mu & d_\mu \end{pmatrix}$ mit der Eigenschaft

$$\begin{pmatrix} a_\nu & b_\nu \\ c_\nu & d_\nu \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a_\mu & b_\mu \\ c_\mu & d_\mu \end{pmatrix}$$

mit einer Modulsubstitution $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Wegen der besonderen Natur des Repräsentantensystems gilt

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}^{-1} \pmod{N}.$$

Dies bedeutet, wenn φ' der $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ entsprechende Automorphismus und σ_μ der $\begin{pmatrix} a_\mu & b_\mu \\ c_\mu & d_\mu \end{pmatrix}$ entsprechende Isomorphismus ist, daß für jedes $g \in L_N$

$$\begin{aligned} g^{\varphi\sigma_\nu}(\tau_0) = g(\sigma_\nu(\varphi(\tau_0))) &= g(\varphi'(\sigma_\mu(\tau_0))) \\ &= g(\sigma_\mu(\tau_0))^{\varphi'} \\ &= (g(\tau_0))^{\sigma_\mu\varphi'} \end{aligned} \tag{16}$$

gilt. Aus (16) folgt sofort, da $L_N = Q(u)$ ist,

$$u^{\varphi\sigma_\nu} = u^{\sigma_\mu\varphi'} \tag{17}$$

und $\varphi' = \tau_n \varphi \tau_n^{-1}$.

Wir sind jetzt in der Lage, den folgenden Satz zu beweisen.

Satz 7. *Es gilt* $X_n \cdot C = C^{\varphi_n^{-1}} \cdot X_n$ *für jede Korrespondenz* C, *die* $\varphi \in S_N$ *zugeordnet ist.*

Beweis. Wenn $u \times u^\varphi$ ein allgemeiner Punkt von C bezüglich $Q(\zeta_N)$ ist, dann folgt aus (11), daß $u^{\varrho_n} \times (u^{\varrho_n})^{\tau_n\varphi\tau_n^{-1}}$ ein allgemeiner Punkt von $C^{\varphi_n^{-1}}$ bezüglich $Q(\zeta_N)$ ist. Wir haben jetzt nach (17)

$$\begin{aligned} (X_n \cdot C)\,(u^{\varrho_n}) = \sum_{\nu=1}^{s} (u^{\varrho_n\varphi})^{\sigma_\nu} &= \sum_{\mu=1}^{s} (u^{\varrho_n\sigma_\mu})^{\tau_n^{-1}\varphi\tau_n} \\ &= C^{\varphi_n^{-1}}\Big(\sum_{\mu=1}^{s} u^{\varrho_n\sigma_\mu}\Big) \\ &= C^{\varphi_n^{-1}}[X_n(u^{\varrho_n})]. \end{aligned}$$

Das heißt aber, daß $X_n \cdot C - C^{\varphi_n^{-1}} \cdot X_n$ von der Form $\mathfrak{A} \times \Gamma_N$ mit einem Divisor $\mathfrak{A}$ auf Γ_N ist. (Weil [13], Th. 2). Da $C^{\varphi_n^{-1}} \cdot X_n$ keine Komponente der Form $\mathfrak{A} \times \Gamma_N$ hat, folgt $\mathfrak{A} > 0$ Aber auf der anderen Seite ist Grad $(X_n \cdot C) =$ Grad $X_n \cdot$ Grad $C =$ Grad X_n, denn es ist Grad $C = 1$. Entsprechend gilt Grad $(C^{\varphi_n^{-1}} \cdot X_n) =$ Grad X_n, so daß $\mathfrak{A} = 0$, d. h. $X_n \cdot C = C^{\varphi_n^{-1}} \cdot X_n$ gilt.

§ 3. Darstellungen von modularen Korrespondenzen.

Sei J eine Jacobische Mannigfaltigkeit der Kurve Γ. Wenn $\Gamma = \Gamma_N$ ist, so bezeichnen wir J mit J_N. Wir dürfen auch annehmen, daß J über Q definiert ist, da Γ über Q definiert ist. Ferner ist auch die kanonische Funktion von Γ in J über Q definiert, weil Γ einen rationalen Punkt über Q hat ([10], S. 23). Nun können die Korrespondenzklassen von Γ mit den Endomorphismen von J identifiziert werden; die letzteren bezeichnen wir mit $\mathfrak{A}(J)$. Die Algebra $\mathfrak{A}(J) \otimes Q$ soll mit $\mathfrak{A}_0(J)$ bezeichnet werden.

Jedem Element $\varphi \in S_N(E)$ haben wir eindeutig eine Korrespondenz C der Kurve Γ über $Q(\zeta_N)$ zugeordnet. Wenn γ diese Korrespondenzklasse bedeutet, dann ist γ als Endomorphismus von J über $Q(\zeta_N)$ definiert. Bezeichnen wir der Einfachheit halber die Gruppe $S_N(E)$ mit S und die Gruppenalgebra von S über $k = Q(\zeta_N)$ mit $R(k)$. Durch eine lineare Erweiterung der Abbildung $\varphi \to \gamma$ läßt sich $R(k)$ in $\mathfrak{A}_0(J) \otimes k$ einbetten.

Jedes Element $\alpha \in \mathfrak{A}(J)$, und insbesondere auch jedes Element der Gruppe S, hat eine Darstellung im Raum der Differentiale erster Gattung von Γ. Da S eine endliche Gruppe ist, zerlegt sich diese Darstellung vollständig in absolut irreduzible Darstellungen über einem gewissen Erweiterungskörper von Q (hier in der Tat über $k = O(\zeta\ )$)

Wir wollen diese Darstellung von $\mathfrak{A}(J)$ mit M^d bezeichnen. Für jedes $\alpha \in S$ gilt

$$M^d(\alpha) \sim \sum_{\chi} M^d(\varepsilon_\chi \cdot \alpha), \tag{18}$$

wo Σ eine direkte Summe und ε_χ die Idempotente, die den irreduziblen Darstellungen der Charaktere χ zugeordnet sind, bedeuten. Die ε_χ sind von der Gestalt

$$\varepsilon_\chi = \frac{r_\chi}{s_0} \sum_{\alpha \in S} \chi(\alpha^{-1}) \cdot \alpha; \tag{19}$$

dabei ist $r_\chi = \chi(1)$ und s_0 die Ordnung von S. Wir werden auch das Bild von $\varepsilon_\chi \in R(k)$ in $\mathfrak{A}_0(J) \otimes k$ mit ε_χ identifizieren.

Nun führt jeder Automorphismus φ_n von $Q(\zeta_N)/Q$ das Element γ in γ^{φ_n} über, und die lineare Erweiterung dieses Automorphismus zu $R(k)$ ergibt einen solchen Automorphismus von $R(k)$, daß $\varepsilon_\chi \to \varepsilon_\chi^{\varphi_n}$ gilt. Man kann $\varepsilon_\chi^{\varphi_n}$ als das Idempotent, das dem Charakter χ^{φ_n} (mit $\chi^{\varphi_n}(\alpha) = \chi(\alpha^{\varphi_n^{-1}})$ zugeordnet ist, betrachten. Denn es ist

$$\begin{aligned}\varepsilon_\chi^{\varphi_n} &= \frac{r_\chi}{s_0} \sum_{\alpha \in S} \chi(\alpha^{-1}) \cdot \alpha^{\varphi_n} = \frac{r_\chi}{s_0} \sum_{\beta} \chi\big((\beta^{\varphi_n^{-1}})^{-1}\big) \\ &= \frac{r_\chi}{s_0} \sum_{\beta \in S} \chi^{\varphi_n}(\beta^{-1}) \cdot \beta = \varepsilon_{\chi^{\varphi_n}},\end{aligned}$$

wo $\alpha^{\varphi_n} = \beta$, oder $\alpha = \beta^{\varphi_n^{-1}}$ ist.

Im allgemeinen ist der Charakter $\chi^{\varphi_n} \neq \chi$ oder, was dasselbe ist, $\varepsilon_\chi^{\varphi_n} \neq \varepsilon_\chi$. Wir teilen die Charaktere χ von S in zwei Klassen ein:

1) $\chi^{\varphi_n} = \chi$ oder $\varepsilon_\chi^{\varphi_n} = \varepsilon_\chi$. In diesem Fall wird χ *vom ersten Typus* genannt.

2) Wenn es unter (χ^{φ_n}) *genau r* verschiedene Charaktere $\chi_1, \ldots, \chi_r$ gibt, dann soll χ *von r-tem Typus* heißen. Für die entsprechenden Idempotente haben wir dann $\varepsilon_{\chi_i} = \varepsilon_\chi^{\varphi_{n_i}}$.

Fall 1. χ *ist vom ersten Typus.* Für soche Charaktere gilt die Gleichung

$$\varepsilon_\chi \cdot \xi_n = \xi_n \cdot \varepsilon_\chi.$$

wo ξ_n die Korrespondenzklasse von X_n ist. Denn es gilt nach Satz 7, wenn $\alpha^{\varphi_n^{-1}} = \beta$ gesetzt wird:

$$\begin{aligned}\xi_n \cdot \varepsilon_\chi &= \frac{r_\chi}{s_0} \sum_{\alpha \in S} \chi(\alpha^{-1}) \cdot \xi_n \cdot \alpha \\ &= \frac{r_\chi}{s_0} \sum_{\alpha} \chi(\alpha^{-1}) \cdot \alpha^{\varphi_n^{-1}} \xi_n \\ &= \frac{r_\chi}{s_0} \sum_{\beta \in S} \chi\big((\beta^{\varphi_n})^{-1}\big) \beta \cdot \xi_n \\ &= \frac{r_\chi}{s_0} \chi^{\varphi_n^{-1}}(\beta^{-1}) \cdot \beta \cdot \xi_n \\ &= \frac{r_\chi}{s_0} \sum_{\beta} \chi(\beta^{-1}) \cdot \beta \cdot \xi_n \\ &= \varepsilon_\chi \cdot \xi_n.\end{aligned}$$

Hieraus folgt, daß die Darstellung $\alpha \to M^d(\varepsilon_\chi \alpha)$ der Algebra $R(k)$ sich zu einer Darstellung der Algebra $\{R(k), \xi_n\}$ (für alle n mit $(n, N) = 1$) erweitern läßt, und zwar durch die Forderung $\xi_n \to M^d(\varepsilon_\chi \xi_n)$. Wir werden jetzt $M^d(\varepsilon_\chi \xi_n)$ explizit ausrechnen und eine Normalform erhalten.

Wenn $\alpha \to M(\alpha)$ eine irreduzible Darstellung mit dem Charakter χ ist, dann ist χ^{φ_n} der Charakter der Darstellung $\alpha \to M(\alpha^{\varphi_n^{-1}})$ zufolge der Definition von χ^{φ_n}. In unserem Fall sind, da $\chi^{\varphi_n} = \chi$ ist, diese beiden Darstellungen mit Koeffizienten in k derart äquivalent, daß

$$M\left(\alpha^{\varphi_n^{-1}}\right) = A_n \cdot M(\alpha) \cdot A_n^{-1} \tag{20}$$

für alle $\alpha \in S$ gilt.

Jetzt ist die Abbildung $\varphi_n \to A_n$ in (20) eine Darstellung der abelschen Gruppe $G(Q(\zeta_n)/Q)$ und läßt sich infolgedessen in 1-dimensionale Darstellungen zerlegen. Mit anderen Worten, für eine passende Basis der Darstellung $\alpha \to M(\alpha)$, können die A_n als Diagonalmatrizen angenommen werden. Wenn $A_n = (\varepsilon_i(n)\, \delta_{ik})$ ist, so liefert die Abbildung $\varphi_n \to \varepsilon_i(n)$ für jedes i eine 1-dimensionale Darstellung von $G(Q(\zeta_N)/Q)$.

Sei fdg eine Differentialform erster Gattung auf der Kurve Γ_N mit $f, g \in \mathfrak{M}_N$. $f(\tau)\, g'(\tau)$ ist dann eine Spitzenform vom Grade —2 und der Stufe N, und umgekehrt ist jede solche Form von diesem Typus. Aus der Definition einer Modulform folgt

$$(fg' \mid L)\ (\tau) = f\left(\frac{a\tau + b}{c\tau + d}\right) \cdot g'\left(\frac{a\tau + b}{c\tau + d}\right) \cdot \frac{1}{(c\tau + d)^2} \tag{21}$$

für eine Modulsubstitution $L = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Wenn φ das entsprechende Element von $L \in S_N(E)$ ist, folgt aus $g^{\varphi}(\tau) = g\left(\frac{a\tau + b}{c\tau + d}\right)$ (für jedes $g \in \mathfrak{L}_N$), daß die Spitzenform $(fg' \mid L)\ (\tau)$ der Differentialform $\delta C(f \cdot dg)$ entspricht (C ist die Korrespondenz, die φ zugeordnet ist). Dabei bedeutet δC das Differential der Korrespondenz C.

Bezeichnet man die Modulsubstitution $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \equiv \begin{pmatrix} n^{-1} & 0 \\ 0 & n \end{pmatrix} \pmod{N}$ mit R_n, dann gilt $g^{\varphi_n}(\tau) = g\left(\frac{\alpha\tau + \beta}{\gamma\tau + \delta}\right)$ für jedes $g \in \mathfrak{L}_N$, denn es ist $\begin{pmatrix} n & 0 \\ 0 & n \end{pmatrix} \equiv \begin{pmatrix} n^2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \pmod{N}$ und $\begin{pmatrix} n^2 & 0 \\ 0 & 1 \end{pmatrix} \in H_N$. Aus der Definition der Korrespondenz Y_n folgt sofort, daß die Darstellung der Y_n oder η_n dieselbe ist wie der Operator R_n.

Ganz entsprechend folgt aus der Definition der „Hecke-Operatoren" T_n ([5], II), für $f, g \in \mathfrak{M}_N$ (fdg eine Differentialform erster Gattung auf Γ_N),

$$(fg' \mid T_n)\ (\tau) = \sum_{\nu=1}^{s} f\left(\frac{a_\nu\tau + b_\nu}{c_\nu\tau + d_\nu}\right) \cdot g'\left(\frac{a_\nu\tau + b_\nu}{c_\nu\tau + d_\nu}\right) \frac{n}{(c_\nu\tau + d_\nu)^2}. \tag{22}$$

Wenn $f, g \in \mathfrak{L}_N$ ist, so folgt nach einem Satz von Shimura ([10], S. 25) und aus den Gleichungen (14), daß die Form $(fg' \mid T_n)$ der Differentialform $(\delta X_n)\ (fdg)$ entspricht, wo δX_n das Differential der Korrespondenz X_n ist.

Infolgedessen sind die Darstellungen $M^d(\gamma)$, $M^d(\xi_n)$ der Korrespondenzklassen von C bzw. X_n dieselben wie die der Operatoren L bzw. T_n im Raum der Spitzenformen vom Grade —2 und der Stufe N. Dasselbe gilt auch für jeden unter einem irreduziblen Bestandteil der Darstellung M^d invarianten Unterraum.

Sei $(F_i(\tau))$ $(i = 1, \ldots, r_\chi)$ ein Spaltenvektor von Spitzenformen, der sich unter der irreduziblen Darstellung D mit dem Charakter χ für die Substitutionen L aus S folgendermaßen transformiert:

$$(F_i) \mid L = M(L) \cdot (F_i). \tag{23}$$

Dann gilt für den Vektor $(F_i) \mid T_n = (G_i)$ nach Satz 5 und (21) und (22):

$$(G_i) \mid L = (F_i) \mid T_n \cdot L = (F_i) \mid L^{\varphi_n^{-1}} \cdot T_n.$$

Die Substitution $L^{\varphi_n^{-1}}$ ist eine Modulsubstitution $L' \equiv S_n L S_n^{-1} \pmod N$ mit $S_n = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$. Aus (23) und (20) folgt ferner, daß

$$A_n^{-1} \cdot (G_i) \mid L = M(L) \cdot A_n^{-1} \cdot (G_i) \tag{24}$$

gilt. Wenn man A_n als Diagonalmatrix annimmt, $A_n = (\varepsilon_i(n) \cdot \delta_{ik})$, so ist $A_n^{-1} = (\bar{\varepsilon}_i(n) \cdot \delta_{ik})$, da $\varepsilon_i^{-1}(n) = \bar{\varepsilon}_i(n)$ ist (die $\varepsilon_i(n)$ sind Einheitswurzeln). (24) impliziert dann: $A_n^{-1}(G_i)$ oder $\bar{\varepsilon}_i(n) \cdot (F_i) \mid T_n$ transformiert sich genau so wie (F_i) bei der Substitution L von S.

Es sei die irreduzible Darstellung $D: L \to M(L)$ $\varkappa$-mal in der ganzen Darstellung M^d enthalten, dann ist $(F_i^\varrho(\tau))$ $(i = 1, \ldots, r_\chi,\ \varrho = 1, \ldots, \varkappa)$ eine Basis des Invariantenraumes unter D. Da $(\bar{\varepsilon}_i(n) F_i^\varrho \mid T_n)$ $(i = 1, \ldots, r_\chi)$ derselben Darstellung D unterliegen, folgt aus der Irreduzibilität von D, daß

$$(\bar{\varepsilon}_i(n) F_i^\varrho) \mid T_n = \sum_{\sigma=1}^{n} \alpha_{\varrho\sigma}(n) F_i^\sigma \qquad (\varrho = 1, \ldots, \varkappa) \tag{25}$$

mit einer $(\varkappa, \varkappa)$-Matrix $\alpha(n) = (\alpha_{\varrho\sigma}(n))$ gilt, deren Elemente in k liegen. $\alpha(n)$ hängt nicht von i ab.

Aus (25) sieht man sofort, daß jedes System $(F_i^{(1)}, \ldots, F_i^{(\varkappa)})$ $(i = 1, \ldots, r_\chi)$ ein Invariantensystem unter allen Operatoren T_n mit $(n, N) = 1$ ist. Wenn man daher alle diese Systeme zusammensetzt, ist die Darstellung von T_n in diesem Invariantenraum äquivalent mit der Matrix

$$\begin{pmatrix} \varepsilon_1(n) \cdot \alpha(n) & 0 & \cdot & \cdot & & 0 \\ 0 & \cdot & & & & \cdot \\ \cdot & & \cdot & & & \cdot \\ \cdot & & & \cdot & & \cdot \\ \cdot & & & & & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & \varepsilon_{r_\chi}(n) \cdot \alpha(n) \end{pmatrix}, \tag{26}$$

wo $\alpha(n)$ wie vorher eine $(\varkappa, \varkappa)$-Matrix mit Elementen aus k und $\varphi_n \to \varepsilon_i(n)$ (für jedes i) eine Darstellung der Gruppe $G(Q(\zeta_N)/Q)$ ist.

Aber auf der anderen Seite ist $M^d(\varepsilon_\chi \xi_n)$ dasselbe wie die Darstellungsmatrix von T_n in diesem Invariantenraum, und so erhalten wir endlich, daß $M^d(\varepsilon_\chi \xi_n)$ äquivalent der Matrix (26) ist.

Aus der Gleichung $M(R_n) \cdot A_n = A_n \cdot M(R_n)$ folgt: Ist A_n Diagonalmatrix, so ist auch $M(R_n)$ Diagonalmatrix, und es gilt sogar $M(R_n) = A_{n^2} \cdot \varepsilon(n)$ mit einer Darstellung $\varphi_n \to \varepsilon(n)$ der Gruppe $G(Q(\zeta_N)/Q)$. Mit anderen Worten, die Darstellung des R_n im vollen Invariantenraum ist die Matrix

$$\begin{pmatrix} \varepsilon_1(n^2) \cdot \varepsilon(n) \cdot E & 0 & \cdot & \cdot & & 0 \\ 0 & \cdot & & & & \cdot \\ \cdot & & \cdot & & & \cdot \\ \cdot & & & \cdot & & \cdot \\ \cdot & & & & & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & \varepsilon_{r_\chi}(n^2) \cdot \varepsilon(n) \cdot E \end{pmatrix}. \tag{26$'$}$$

Aber wie wir schon bemerkt haben, ist $M^d(\varepsilon_\chi \eta_n)$ dieselbe Matrix wie die Darstellungsmatrix von R_n, d. h. $M^d(\varepsilon_\chi \eta_n) \sim (26)'$.

Fall II. *χ ist vom r-ten Typus* ($r > 1$). Hier betrachten wir den imprimitiven Charakter $\chi_0 = \sum_{i=1}^{r} \chi_i$, der die Eigenschaft $\chi_0^{\varphi_n} = \chi_0$ für alle φ_n mit $(n, N) = 1$ hat. Mit anderen Worten gilt auch $\varepsilon_{\chi_0}^{\varphi_n} = \varepsilon_{\chi_0}$, und wie in (20) gilt $\varepsilon_{\chi_0} \cdot \xi_n = \xi_n \cdot \varepsilon_{\chi_0}$.

Nehmen wir an, daß $\chi_1 = \chi$ ist und $\chi_l = \chi_1^{\varphi_{n_l}}$ $(1 \leqq l \leqq r)$. Wir bemerken ferner, daß $\chi_l(1) = \chi(1) = r_\chi$ für alle l ist. Bezeichnen wir mit U die Untergruppe von (φ_n), die χ_1 fixieren, d. h. die Untergruppe aller φ_λ, für die $\chi_1^{\varphi_\lambda} = \chi_1$ gilt. Wie im Fall I gibt es für jedes λ $(\varphi_\lambda \in U)$ eine Matrix A_λ mit Elementen in k mit der Eigenschaft

$$M(\alpha^{\varphi_\lambda^{-1}}) = A_\lambda \cdot M(\alpha) \cdot A_\lambda^{-1}, \tag{27}$$

wo $M(\alpha)$ Element der Darstellung D_1 mit dem Charakter χ_1 ist. A_λ kann man als Diagonalmatrix annehmen und wenn $A_\lambda = (\varepsilon_i(\lambda) \cdot \delta_{ik})$ ist, wird $\varphi_\lambda \to \varepsilon_i(\lambda)$ eine Darstellung der Gruppe U. Durch direkte Rechnung folgt wie im Fall I (Hecke, [5], II, Satz 47a): Wenn die Formen (F_i) $(i = 1, \ldots, r_\chi)$ der Darstellung D_1 unterliegen (D_1 mit Charakter χ_1), so gibt es λ und v derart, daß die Formen $(\bar{\varepsilon}_i(\lambda) F_i) \mid T_n$ der Darstellung D_v (mit Charakter χ_v) unterliegen, wo v, λ und l folgendermaßen zusammenhängen:

$$\varphi_\lambda = \varphi_n \cdot \varphi_{n_l} \cdot \varphi_{n_v}^{-1} \qquad (\varphi_\lambda \in U).$$

Bezeichnen wir mit $\varkappa_i$ die Vielfachheit von D_i in der Darstellung M^d. Wenn (F_i^ϱ) $(i = 1, \ldots, r_\chi,\ \varrho = 1, \ldots, \varkappa_l)$ und (H_i^σ) $(i = 1, \ldots, r_\chi,\ \sigma = 1, \ldots, \varkappa_v)$ die Basen der vollen Invariantenräume von D_l und D_v sind, dann erhalten wir wegen der Irreduzibilität von D_l und D_v:

$$\bar{\varepsilon}_i(\lambda) F_i^\varrho \mid T_n = \sum_{\sigma=1}^{\varkappa} \alpha_{\varrho\sigma}(\lambda) H_i^\sigma \quad (i = 1, \ldots, r_\chi,\ \varrho = 1, \ldots, \varkappa_l), \tag{28}$$

wo $\alpha(\lambda) = (\alpha_{\varrho\sigma}(\lambda))$ eine $(\varkappa_l, \varkappa_v)$-Matrix mit von i unabhängigen Elementen aus k ist. Nun betrachten wir die direkte Summe all dieser Invariantenräume; das ist ein Raum der Dimension $r_{\chi_1}(\sum_{i=1}^{r} \varkappa_i) = r_{\chi_1} \cdot \varkappa$. Er läßt sich zerlegen in r_χ Systeme $(F_i^1, \ldots, F_i^{\varkappa_l}, G_i^1, \ldots, H_i^1, \ldots, H_i^{\varkappa_v}, \ldots)$ $(i = 1, \ldots, r_\chi)$. Aus (28) folgt, daß jedes System unter allen Operatoren T_n invariant bleibt, so daß die Darstellung von T_n in dieser direkten Summe D_0 äquivalent mit der Matrix

$$\left(\begin{array}{cccc} \boxed{\begin{matrix} \varepsilon_1(\lambda_1)\,\alpha(\lambda_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \varepsilon_{r_\chi}(\lambda_1)\,\alpha(\lambda_1) \end{matrix}} & & & \\ & \boxed{\begin{matrix} \varepsilon_1(\lambda_2)\,\beta(\lambda_2) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \varepsilon_{r_\chi}(\lambda_2)\,\beta(\lambda_2) \end{matrix}} & & \\ & & \ddots & \\ & & & \ddots \end{array}\right) \tag{29}$$

ist, wenn man alle diese Darstellungen zusammensetzt; λ_i ist so gewählt, daß $\varphi_{\lambda_i} \in U$ ist.

Andererseits aber ist $M^d(\varepsilon_{\chi_0} \xi_n)$ dasselbe wie die Darstellungsmatrix von T_n im vollen Invariantenraum D_0, so daß $M^d(\varepsilon_{\chi_0} \xi_n)$ äquivalent zu der Matrix (29) ist.

Ferner folgt wie im Fall I wegen der Beziehung $M_l(R_n) \cdot A_\lambda = A_\lambda \cdot M_l(R_n)$ für jedes l, daß $M_l(R_n) = A_{\lambda^n} \cdot \varepsilon(\lambda)$ ist, wo $\varphi_\lambda \to \varepsilon(\lambda)$ eine Darstellung der Gruppe U ist. Da λ von n und l abhängig ist, erhalten wir für die Darstellung der R_n im vollen Invariantenraum D_0 die Matrix

$$(29') \qquad \begin{pmatrix} \boxed{\begin{matrix} \varepsilon_1^2(\lambda_1)\,\varepsilon(\lambda_1)\,E & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \varepsilon_{r_\chi}^2(\lambda_1)\,\varepsilon(\lambda_1)\,E \end{matrix}} & & \\ & \boxed{\begin{matrix} \varepsilon_1^2(\lambda_2)\,\varepsilon(\lambda_2)\,E & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \varepsilon_{r_\chi}^2(\lambda_2)\,\varepsilon(\lambda_2)\,E \end{matrix}} & \\ & & \ddots \end{pmatrix}$$

Aus unseren Bemerkungen folgt dann, daß $M^d(\varepsilon_{\chi_0}\eta_n)$ äquivalent zu der Matrix (29′) ist.

Teil II.

§ 4. Reduktionstheorie.

In diesem Abschnitt erhalten wir weitere Korrespondenzrelationen durch die Anwendung der Reduktionstheorie von Deuring und Shimura ([1], [8]) und benutzen diese Relationen zum Studium der Struktur von L-Reihen, die mit $K_N(E)$ verknüpft sind.

Sei k ein algebraischer Zahlkörper und $\mathfrak{p}$ ein Primideal in k. Wir bezeichnen mit $\tilde{k}$ den Restklassenkörper von k modulo $\mathfrak{p}$. Bedeutet $\mathfrak{X}$ ein algebraisch-geometrisches Objekt, definiert bezüglich k, so soll $\mathfrak{X}(\mathfrak{p})$ oder $\tilde{\mathfrak{X}}$ die Reduktion von $\mathfrak{X}$ modulo $\mathfrak{p}$ bedeuten.

Sei V eine vollständige singularitätenfreie Mannigfaltigkeit bezüglich k. Nach Shimura heißt ein Primdivisor $\mathfrak{p}$ *ohne Defekt für* V, wenn die folgenden Bedingungen erfüllt sind [8]:

a) V ist $\mathfrak{p}$-einfach,

b) V ist $\mathfrak{p}$-vollständig,

c) V hat keine singulären Punkte.

Wenn das der Fall ist, so haben, wenn V eine Kurve ist, V und $\tilde{V}$ dasselbe Geschlecht. Ferner hat V im Fall einer elliptischen Kurve, als abelsche Mannigfaltigkeit, keinen Defekt für $\mathfrak{p}$.

Seien Γ, Γ' zwei über k definierte vollständige Kurven ohne singuläre Punkte und X eine bezüglich k rationale Korrespondenz zwischen Γ und Γ'. Durch Reduktion modulo $\mathfrak{p}$ ($\mathfrak{p}$ ein Primdivisor in k ohne Defekt für Γ, Γ') erhält man eine Korrespondenz $\tilde{X} = X(\mathfrak{p})$ zwischen $\tilde{\Gamma}$ und $\tilde{\Gamma}'$. Wenn ferner J, J' die Jacobischen Mannigfaltigkeiten von Γ und Γ' sind, so sind die reduzierten Mannigfaltigkeiten $\tilde{J}$ und $\tilde{J}'$ die Jacobischen Mannigfaltigkeiten von $\tilde{\Gamma}$ und $\tilde{\Gamma}'$; außerdem sind $\tilde{J}$, $\tilde{J}'$ über $\tilde{k}$ definiert. Wenn der X zugeordnete Homomorphismus von J in J' mit ξ bezeichnet wird, dann ist $\tilde{\xi}$ der $\tilde{X}$ zugeordnete Homomorphismus von $\tilde{J}$ in $\tilde{J}'$. Wenn $J = J'$ ist, so ist die Abbildung $\xi \to \tilde{\xi}$ ein Isomorphismus von $\mathfrak{A}(J)$ in $\mathfrak{A}(\tilde{J})$.

Wie in Teil I sei L ein Unterkörper von K_N derart, daß $L > Q(j_0)$, $L \frown Q(\zeta_N) = Q$ ist. Sei Γ eine Kurve mit $L = Q(u)$ und u ein allgemeiner Punkt von Γ bezüglich Q. Sei $n = p$ eine Primzahl ($p \nmid N$). Nach Deuring und Shimura hat Γ keinen Defekt für fast alle Primzahlen p; sei p eine dieser Primzahlen. Für jede dieser Primzahlen p fixieren wir eine der Erweiterungen (als Bewertung) in F, der algebraisch-abgeschlossenen Hülle von $Q(j_0)$ und nennen sie auch p. Bezeichnet $\tilde{u}$ den reduzierten Punkt von u, dann gilt $\tilde{Q}(\tilde{u}) = \tilde{L}$, und $\tilde{u}$ ist ein allgemeiner Punkt von $\tilde{\Gamma}$ bezüglich $\tilde{Q}$.

Sei $\Pi(p)$ der Ort von $\tilde{u} \times \tilde{u}^p$ auf $\tilde{\Gamma} \times \tilde{\Gamma}$ in bezug auf $\tilde{Q}$. Dann gilt nach Shimura ([10], S. 16) zwischen $\tilde{X}_p$, $\tilde{Y}_p$ und $\Pi(p)$ die folgende Beziehung:

$$\tilde{X}_p = \Pi(p) + \Pi(p)' \cdot \tilde{Y}_p. \tag{30}$$

Ferner erhalten wir aus Satz 6 durch Reduktion modulo p:

$$\tilde{A}^{\varphi_p} \cdot \tilde{Y}_p = \tilde{A}.$$

Aber da φ_p der Frobeniussche Automorphismus $\left(\frac{Q(\zeta_N)/Q}{p}\right)$ ist, so kann diese Gleichung auch in der Form

$$\tilde{A}^p \cdot \tilde{Y}_p = \tilde{A}$$

geschrieben werden. Aus den Gleichungen $\tilde{A}' \cdot \tilde{A} = \tilde{\Delta}$ (da $\tilde{A}$ eine birationale Korrespondenz ist; $\tilde{\Delta}$ die Diagonale von $\tilde{\Gamma} \times \tilde{\Gamma}$) und $\tilde{A} \cdot \Pi(p)' = \Pi(p)' \cdot \tilde{A}^p$ erhalten wir

$$A \cdot \Pi(p)' \cdot \tilde{A} = \tilde{A}' \cdot \Pi(p)' \cdot \tilde{A}^p \cdot \tilde{Y}_p = \tilde{A}' \cdot \tilde{A} \cdot \Pi(p)' \cdot \tilde{Y}_p = \Pi(p)' \cdot \tilde{Y}_p. \tag{31}$$

Sei J eine Jacobische Mannigfaltigkeit von Γ und φ eine kanonische Funktion von Γ in J. Da Γ über Q definiert ist, kann J auch über Q definiert werden, und da Γ einen rationalen Punkt über Q hat, können wir auch φ über Q definieren. Bedeuten ξ_n bzw. η_n die Korrespondenzklassen von X_n bzw. Y_n, so ist $\xi_n, \eta_n \in \mathfrak{A}(J)$. Für fast alle Primzahlen p hat J keinen Defekt für p, so daß $\tilde{J}$ die Jacobische Mannigfaltigkeit von $\tilde{\Gamma}$ und $\tilde{\varphi}$ eine kanonische Funktion von $\tilde{\Gamma}$ in $\tilde{J}$ ist. Wenn weiter ξ_n und η_n in $\tilde{\xi}_n$, $\tilde{\eta}_n$ übergehen, so ist $\tilde{\xi}_n, \tilde{\eta}_n \in \mathfrak{A}(\tilde{J})$ und es gelten die Gleichungen

$$\begin{aligned} \tilde{\xi}_p &= \pi(p) + \pi(p)' \cdot \tilde{\eta}_p, \\ \pi(p)' \cdot \tilde{\eta}_p &= \tilde{\alpha}^{-1} \cdot \pi(p)' \cdot \tilde{\alpha}, \end{aligned} \tag{32}$$

wo die letztere auf $\tilde{\Gamma}_N$ gilt, α die Korrespondenzklasse von A und $\pi(p)$ die Klasse von $\Pi(p)$ ist.

Bezeichnen wir jetzt mit $Q(J)$ den über Q definierten rationalen Funktionenkörper von J oder, was dasselbe ist, den abelschen Funktionenkörper, der K zugeordnet ist. Dann kann man leicht einsehen, daß der K_N zugeordnete abelsche Funktionenkörper nichts anderes als $Q(\zeta_N)(J) = Q(J)(\zeta_N)$ ist: es ist $Q(J) = Q(u_1, \ldots, u_g)_s$, wo $u_1, \ldots, u_g$ g unabhängige allgemeine Punkte von Γ bezüglich Q sind; $Q(u_1, \ldots, u_g)_s$ ist derjenige Unterkörper von $Q(u_1, \ldots, u_g)$, der unter allen Automorphismen von $Q(u_1, \ldots, u_g)$ invariant bleibt, die Q fixieren und $(u_1, \ldots, u_g)$ permutieren. Da Q in $Q(u_1, \ldots, u_g)$ algebraisch abgeschlossen ist, folgt

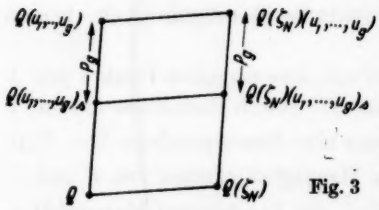


Fig. 3

$$\begin{aligned} Q(\zeta_N)(J) &= (Q(\zeta_N)(u_1, \ldots, u_g))_s \\ &= Q(u_1, \ldots, u_g)_s \cdot Q(\zeta_N) \\ &= Q(J)(\zeta_N). \end{aligned}$$

Für eine Primzahl p, für die J keinen Defekt hat, läßt sich p zu einem Funktionalprimdivisor $p_{Q(J)}$ von $Q(J)$ erweitern, der außerdem *einfach* ist (im Sinne von Deuring, [3]). Indem wir den Satz 1 von Deuring in [3] auf den Fall $K = Q(J)$, $k = Q$, $k_1 = Q(\zeta_N)$ anwenden, sehen wir, daß wir zu jedem Primteiler P von p in $Q(\zeta_N)$ eine Erweiterung $P_{Q(\zeta_N)(J)}$ erhalten, da $Q(J)$ über Q und $\widetilde{Q(J)}$ über $\widetilde{Q}$ regulär ist. Der Primdivisor $P_{Q(\zeta_N)(J)}$ ist über $Q(\zeta_N)$ einfach; $\widetilde{Q(\zeta_N)\,(J)}$ ist regulär über $\widetilde{Q(\zeta_N)}$, und es gilt $\widetilde{Q(\zeta_N)(J)} = \widetilde{Q(J)} \cdot \widetilde{Q(\zeta_N)}$.

Nun definieren wir nach Roquette [7] einen *Meromorphismus* eines abelschen Funktionenkörpers A als einen Isomorphismus η von A in seine algebraisch-abgeschlossene Hülle $\bar{A}$, und er ist *vom ersten Grade*, wenn das Bild $A\eta < A$ liegt. Ein *regulärer Multiplikator* (im Sinne von Hasse) von $\widetilde{K}$ (oder $\widetilde{K}_N$) induziert einen Meromorphismus ersten Grades von $\widetilde{Q(J)}$ (oder $\widetilde{Q(\zeta_N)\,(J)}$), und nach dem Äquivalenzsatz von Roquette [7] erhält man eine 1 — 1-Korrespondenz zwischen regulären Multiplikatoren von $\widetilde{K}$ (oder $\widetilde{K}_N$) und Meromorphismen ersten Grades von $\widetilde{Q(J)}$ (oder $\widetilde{Q(\zeta_N)\,(J)}$).

Wir führen einen Hilfsbegriff, *den verallgemeinerten Meromorphismus*, ein. Wenn A ein abelscher Funktionenkörper über k und σ ein Automorphismus von k ist, dann definieren wir einen *verallgemeinerten Meromorphismus* Σ als einen Isomorphismus von A auf einen Unterkörper A^{Σ}, der auf k mit dem gegebenen Automorphismus σ übereinstimmt. (Für elliptische Funktionenkörper siehe Deuring [2].)

Sei φ_n der Automorphismus von $Q(\zeta_N)/Q$, der ζ_N in ζ_N^n überführt. Dann läßt sich φ_n zu einem Automorphismus von $Q(\zeta_N)\,(J)$ erweitern, indem man $\alpha^{\varphi_n} = \alpha$ für $\alpha \in Q(J)$ setzt. Wir bezeichnen diesen verallgemeinerten Meromorphismus mit Φ_n.

Nun folgt aus $\tau'_n \in H_N$, daß $u^{\tau'_n} = u$ gilt. Das impliziert dann $\alpha^{\tau'_n} = \alpha$ für alle $\alpha \in Q(J)$. Ferner ist $\tau'_n = \varphi_n$ auf $Q(\zeta_N)$, so daß $\beta^{\tau'_n} = \beta^{\varphi_n}$ für $\beta \in Q(\zeta_N)$ gilt. Aus diesen beiden Gleichungen erhalten wir die Aussage, daß die Erweiterung von τ'_n zu $Q(\zeta_N)\,(J)$ genau der verallgemeinerte Meromorphismus Φ_n ist.

Für jeden Multiplikator $\mu \in S$ (d. h. die den Elementen von S zugeordnet sind) von K_N gilt der folgende Satz:

Satz 8. *Es gilt* $\Phi_n \cdot \mu \cdot \Phi_n^{-1} = \mu^{\varphi_n}$ (μ^{φ_n} *wie in Teil I*).

Beweis. Da beides Multiplikatoren von K_N sind, sind sie die Identität auf $Q(\zeta_N)$. Es genügt daher, die Gleichung auf $Q(J)$ zu betrachten. Nun folgt aus Satz 5, daß $\alpha^{\mu^{\varphi_n}} = \alpha^{\tau'_n \cdot \mu \cdot \tau'^{-1}_n}$ für jedes $\alpha \in Q(J)$ ist. Da τ'_n den verallgemeinerten Meromorphismus Φ_n induziert, bedeutet diese Gleichung $\alpha^{\mu^{\varphi_n}} = \alpha^{\Phi_n \mu \Phi_n^{-1}}$ für $\alpha \in Q(J)$.

Für $n = p$ gilt $P^{\varphi_p} = P$ für jeden Primteiler P von p in $Q(\zeta_N)$, da φ_p der Frobeniussche Automorphismus $\left(\frac{(Q(\zeta_N)/Q)}{p}\right)$ ist. Wenn also $\boldsymbol{P}$ den erweiterten Primdivisor von P und $p_{Q(J)}$ zu $Q(\zeta_N)\,(J)$ bedeutet, ist der Primdivisor $\boldsymbol{P}^{\varphi_p}$ gleich $\boldsymbol{P}$. Mit anderen Worten, der verallgemeinerte Meromorphismus Φ_p geht in einen verallgemeinerten Meromorphismus $\widetilde{\Phi}_p$ von $\widetilde{Q(\zeta_N)\,(J)}$ über $\widetilde{Q(\zeta_N)}_P$ über.

Nun ist $\widetilde{\varphi}_p$ der Automorphismus $\alpha \to \alpha^p$ auf $\widetilde{Q(\zeta_N)}$, so daß die Abbildung $\alpha \to \alpha^p$ von $\widetilde{Q(\zeta_N)\,(J)}$ ein verallgemeinerter Meromorphismus π_0 ist. Mit $(\widetilde{Q(\zeta_N)}_P : \widetilde{Q}_p) = f_p$ setzen wir $\pi^* = \pi_0 \cdot \widetilde{\Phi}_p^{f_p - 1}$. Dann ist der verallgemeinerte Meromorphismus π^* ein Meromorphismus ersten Grades, da er eingeschränkt auf $\widetilde{Q(\zeta_N)}$ die Identität ist. Aus unseren Bemerkungen folgt dann, daß π^* als ein Multiplikator von $\widetilde{K}_N$ betrachtet werden kann. Weil π^*, eingeschränkt auf $\widetilde{Q(J)}$, der Meromorphismus $\alpha \to \alpha^p$ ist, gilt $\pi^* = \pi(p)$ auf $\widetilde{Q(J)}$.

Durch Reduktion modulo P (in $Q(\zeta_N)$) folgt nach Satz 8 sofort (für $n = p$)

$$\tilde{\mu}^{\tilde{\varphi}_p} = \tilde{\Phi}_p \cdot \tilde{\mu} \cdot \tilde{\Phi}_p^{-1} \tag{33}$$

für jedes $\mu \in S$. Es ist aber

$$\pi^{*-1}\tilde{\mu}\pi^* = \tilde{\Phi}_p \pi_0^{-1}\tilde{\mu}\pi_0\tilde{\Phi}_p^{-1} = \Phi_p\tilde{\mu}\tilde{\Phi}_p^{-1};$$

denn es gilt $\tilde{\Phi}_p^{\prime p-1} = \tilde{\Phi}_p^{-1}$, und $\pi_0\mu = \tilde{\mu}\pi_0$. Mit anderen Worten: Es gilt

$$\pi^{*-1}\tilde{\mu}\pi^* = \tilde{\mu}^{\tilde{\Phi}_p^{-1}}. \tag{34}$$

Mit einem einfachen Charakter χ der Gruppe S erhalten wir wie in Teil I das Idempotent $\varepsilon_\chi (\in \mathfrak{A}_0(J) \otimes k)$, und wir bezeichnen mit $\tilde{\varepsilon}_\chi$ das Element $\tilde{\varepsilon}_\chi = \frac{r_\chi}{s_0} \sum_{\alpha \in S} \chi(\alpha^{-1}) \cdot \tilde{\alpha}$, wo $\tilde{\alpha}$ der reduzierte Multiplikator von α ist. Wie vorhin unterscheiden wir zwei Fälle.

Fall I: *χ ist vom ersten Typus.* In diesem Fall gilt $\chi^{\varphi_p} = \chi$, d. h. $\tilde{\varepsilon}_\chi^{\tilde{\varphi}_p^{-1}} = \tilde{\varepsilon}_\chi$. Aus (34) folgt dann

$$\pi^{*-1}\tilde{\varepsilon}_\chi\pi^* = \tilde{\varepsilon}_\chi^{\tilde{\varphi}_p^{-1}} = \tilde{\varepsilon}_\chi \tag{35}$$

oder

$$\tilde{\varepsilon}_\chi\pi^* = \pi^*\tilde{\varepsilon}_\chi.$$

Wenn man $\tilde{\varepsilon}_\chi$ auf den Körper $\widetilde{Q(J)}$ einschränkt, impliziert (35) die Gleichung

$$\pi(p) \cdot \tilde{\varepsilon}_\chi = \tilde{\varepsilon}_\chi \cdot \pi(p), \tag{36}$$

da $\pi^* = \pi(p)$ auf $\widetilde{Q(J)}$ ist.

Fall II: *χ ist vom r-ten Typus* ($r > 1$). Setzen wir $\chi_0 = \sum_{i=1}^{r} \chi_i$. $\varepsilon_{\chi_0}^{\varphi_p} = \varepsilon_{\chi_0}$ bedeutet dann $\tilde{\varepsilon}_{\chi_0}^{\tilde{\varphi}_p^{-1}} = \tilde{\varepsilon}_{\chi_0}$. Wieder folgt aus (34), daß

$$\pi^{*-1}\varepsilon_{\chi_0}\pi^* = \tilde{\varepsilon}_{\chi_0}^{\tilde{\varphi}_p^{-1}} = \tilde{\varepsilon}_{\chi_0}$$

oder

$$\pi^*\tilde{\varepsilon}_{\chi_0} = \tilde{\varepsilon}_{\chi_0}\pi^*$$

gilt. Indem wir diese Gleichung auf $\widetilde{Q(J)}$ betrachten, erhalten wir endlich

$$\pi(p) \cdot \tilde{\varepsilon}_{\chi_0} = \tilde{\varepsilon}_{\chi_0} \cdot \pi(p). \tag{37}$$

§ 5. Artinsche L-Reihen.

Die folgenden Sätze 9 und 10 gelten allgemein für eine Galoissche Erweiterung.

Der Körper $\tilde{K}_N$ ist eine Galoissche Erweiterung von $\widetilde{Q(j_0, \zeta_N)} = \tilde{R}_N$ mit zu S isomorpher Galoisgruppe (das folgt aus der Reduktionstheorie). Folglich können wir zu jedem χ von S die Artinsche L-Reihe von $\tilde{K}_N/\tilde{R}_N$ definieren (S. 81 [13]).

Definitionsgemäß ist $L_\chi(u)$ eine analytische Funktion von u, die für $u = 0$ den Wert 1 annimmt und in der Umgebung von $u = 0$ von folgender Gestalt ist:

$$L_\chi(u) = \frac{\exp\left(-\int_0^u \Phi_\chi(u)\,\frac{du}{u}\right)}{(1-u)^{\varrho_\chi}(1-p'^p u)^{\varrho_\chi}}, \tag{38}$$

wobei p^{f_p} die Anzahl der Elemente von $\overline{Q(\zeta_N)}$ und

$$\varrho_\chi = \begin{cases} 1 \text{ wenn } \chi = 1 \\ 0 \text{ wenn } \chi \neq 1 \end{cases}$$

ist. Φ_χ ist folgendermaßen definiert:

$$\Phi_\chi(u) = \frac{1}{r_\chi} \sum_{n=1}^{\infty} \sigma(\tilde{\varepsilon}_\chi \iota^n) \cdot u^n,$$

wo σ die Spur der l-adischen Darstellung M_l der Multiplikatoren von $\tilde{K}_N$ und ι die Korrespondenzklasse von $\alpha \to \alpha^{p^{f_p}}$ (auf $\tilde{K}_N$) ist.

Wir werden jetzt folgenden Satz beweisen.

Satz 9. *Für* $\chi \neq 1$ *gilt* $L_\chi(u) = | E - M_l(\tilde{\varepsilon}_\chi \cdot \iota) \cdot u |$ (dabei ist E die Einheitsmatrix).

Beweis. Sei $| E - M_l(\tilde{\varepsilon}_\chi \cdot \iota) \cdot u | = \prod_{i=1}^{2g} (1 - \alpha_i u)$, wo α_i die charakteristischen Wurzeln von $M_l(\tilde{\varepsilon}_\chi \iota)$ sind. Dann gilt

$$\begin{aligned} -\log | E - M_l(\tilde{\varepsilon}_\chi \iota) \cdot u | &= -\sum_{i=1}^{2g} \log (1 - \alpha_i u) \\ &= \sum_{i=1}^{2g} \sum_{n=1}^{\infty} \frac{(\alpha_i u)^n}{n} \\ &= \sum_{n=1}^{\infty} \left(\sum_{i=1}^{2g} \alpha_i^n \right) \frac{u^n}{n}. \end{aligned}$$

Aus den Sätzen von Weil [13] schließt man, daß die α_i nichts anderes sind als die λ_i je mit der Vielfachheit a_i, wo die λ_i, a_i folgendermaßen erklärt sind:

$$\tilde{\varepsilon}_\chi \iota = \sum_i \lambda_i \varepsilon_i; \ (\tilde{\varepsilon}_\chi = \sum_i \varepsilon_i) \text{ und } \sigma(\varepsilon_i) = a_i.$$

Ferner folgt

$$\tilde{\varepsilon}_\chi \iota^n = \sum \lambda_i^n \cdot \varepsilon_i, \ \sigma(\tilde{\varepsilon}_\chi \iota^n) = \sum_i a_i \lambda_i^n,$$

was bedeutet, daß die charakteristischen Wurzeln von $M_l \tilde{\varepsilon}_\chi(\iota^n)$ die λ_i^n, jede mit Vielfachheit a_i, sind. Mit anderen Worten: es ist

$$\sum_i \alpha_i^n = \sum_i a_i \lambda_i^n = \sigma(\tilde{\varepsilon}_\chi \iota^n).$$

Also folgt

$$\begin{aligned} -\log | E - M_l(\tilde{\varepsilon}_\chi \iota) \cdot u | &= \sum_{n=1}^{\infty} \sigma(\tilde{\varepsilon}_\chi \iota^n) \cdot \frac{u^n}{n}, \\ -\frac{d}{du} \log | E - M_l(\tilde{\varepsilon}_\chi \iota) \cdot u | &= \frac{1}{u} \sum_{n=1}^{\infty} \sigma(\tilde{\varepsilon}_\chi \iota^n) \cdot u^n \\ &= \frac{1}{u} \Phi_\chi(u) \cdot r_\chi. \end{aligned}$$

Nach einer Umrechnung erhalten wir aus (38) (für $\chi \neq 1$)

$$(L_\chi(u))^{r_\chi} = | E - M_l(\tilde{\varepsilon}_\chi \iota) \cdot u |. \tag{39}$$

Bemerkung. Für einen imprimitiven Charakter $\chi_0 = \sum_{i=1}^{r} \chi_i$ mit der Eigenschaft $r_{\chi_i} = r_\chi$ (für alle i) folgt dann ohne weiteres

$$\prod_{i=1}^{r} (L_{\chi_i}(u))^{r_\chi} = (L_{\chi_0}(u))^{r_\chi} = | E - M_l(\tilde{\varepsilon}_{\chi_0} \iota) \cdot u |. \tag{39'}$$

Satz 10. *Bezeichnet $Z(u)$ die Zetafunktion des Körpers $\widetilde{K}_N$, dann gilt*

$$Z(u) = \prod_{\chi} (L_\chi(u))^{r_\chi},$$

wo das Produkt über alle einfachen Charaktere χ von S läuft.

Beweis. Aus der Beziehung $1 = \sum_{\chi} \tilde{\varepsilon}_\chi$ folgt $\sigma(\iota^n) = \sum_{\chi} \sigma(\tilde{\varepsilon}_\chi \iota^n)$. Nun ist ([13], S. 70)

$$\begin{aligned} d(\log P(u)) &= -\sum_{n=1}^{\infty} \sigma(\iota^n) \cdot u^n \cdot \frac{du}{u} \\ &= -\sum_{\chi} \sum_{n=1}^{\infty} \sigma(\tilde{\varepsilon}_\chi \iota^n) \cdot u^n \cdot \frac{du}{u} \\ &= -\sum_{\chi} r_\chi \cdot \Phi_\chi(u) \cdot \frac{du}{u}. \end{aligned}$$

Durch Integration und Erhebung in die Exponentialpotenz erhält man auf beiden Seiten:

$$P(u) = \prod_{\chi} e^{-\int_0^u r_\chi \Phi_\chi(u) \frac{du}{u}} = \prod_{\substack{\chi \\ (\chi \neq 1)}} (L_\chi(u))^{r_\chi} (L_1(u)) (1-u)(1-p^{f_p} \cdot u)$$

oder

$$Z(u) = \frac{P(u)}{(1-u)(1-p^{f_p} \cdot u)} = \prod_{\chi} (L_\chi(u))^{r_\chi}. \tag{40}$$

Aus den Gleichungen (32), (36) und (37) erhalten wir mit einer Unbestimmten u

$$\begin{aligned} &| E - M_l(\tilde{\varepsilon}_\chi \cdot \tilde{\xi}_p) + M_l(\tilde{\varepsilon}_\chi \cdot \tilde{\eta}_p) \cdot p \cdot u^2 | \\ &\quad = | E - M_l(\tilde{\varepsilon}_\chi \pi(p)) \cdot u | \cdot | E - M_l(\tilde{\varepsilon}_\chi \pi(p)' \cdot \tilde{\eta}_p) \cdot u |, \end{aligned}$$

wo χ entweder χ oder χ_0 bedeuten soll, je nachdem, ob χ vom ersten oder r-ten Typus ist. Aus (32) folgt aber

$$M_l(\tilde{\varepsilon}_\chi \pi(p)' \cdot \tilde{\eta}_p) \sim M_l(\tilde{\varepsilon}_\chi \pi(p)') \sim M_l(\tilde{\varepsilon}_\chi \pi(p)),$$

so daß

$$| E - M_l(\tilde{\varepsilon}_\chi \cdot \tilde{\xi}_p) \cdot u + M_l(\tilde{\varepsilon}_\chi \cdot \tilde{\eta}_p) \cdot pu^2 | = | E - M_l(\tilde{\varepsilon}_\chi \pi(p)\, u |^2 \tag{41}$$

gilt.

Wir können jetzt die l-adische Darstellung von $\mathfrak{A}_0(J) \otimes k$ so wählen, daß $M_l(\alpha) = M_l(\tilde{\alpha})$ gilt. Ferner ist $M_l \sim \overline{M}^d \oplus M^d$, wo M^d wie vorher die Darstellung durch die Differentiale erster Gattung bedeutet und $\overline{M}^d$ die konjugiert Komplexe zu M^d ist.

Es folgt daraus:

$$\begin{aligned} &| E - M_l(\tilde{\varepsilon}_\chi \cdot \tilde{\xi}_p) \cdot u + M_l(\tilde{\varepsilon}_\chi \cdot \tilde{\eta}_p) \cdot pu^2 | \\ &\quad = | E - M_l(\varepsilon_\chi \xi_p) \cdot u + M_l(\varepsilon_\chi \eta_p) \cdot pu^2 | \\ &\quad = | E - M^d(\varepsilon_\chi \xi_p)\, u + M^d(\varepsilon_\chi \eta_p)\, pu^2 | \\ &\qquad \cdot | E - \overline{M^d(\varepsilon_\chi \xi_p)}\, u + \overline{M^d(\varepsilon_\chi \eta_p)} \cdot pu^2 |. \end{aligned}$$

Insbesondere gilt für einen reellen Charakter χ, da ξ_p, η_p und J über Q definiert sind und $M^d(\varepsilon_\chi \alpha)$ für $\alpha \in S$ in $Q(\chi)$ realisierbar ist [6], daß sich $M^d(\varepsilon_\chi \xi_p)$ und $M^d(\varepsilon_\chi \eta_p)$ in $Q(\chi)$ realisieren lassen, und zwar so, daß

$$\overline{M^d(\varepsilon_\chi \xi_p)} = M^d(\varepsilon_\chi \xi_p) \text{ und } \overline{M^d(\varepsilon_\chi \eta_p)} = M^d(\varepsilon_\chi \eta_p) \text{ ist.}$$

In diesem Fall folgt dann aus (41):

$$| E - M_l(\varepsilon_\chi \pi(p)) \cdot u | = | E - M^d(\varepsilon_\chi \xi_p) \cdot u + M^d(\varepsilon_\chi \eta_p)\, pu^2 |. \tag{42}$$

(Wir beschränken uns nur auf solche Fälle, wo χ oder χ_0, wenn χ vom r-ten Typus ist, reell sind.)

Da der Multiplikator ι von K_N durch die Abbildung $\alpha \to \alpha^{p^f p}$ induziert wird, so gilt $\iota = \pi_0^{f_p} = \pi^{*f_p}$, weil $\tilde{\Phi}_p^{f_p} = 1$ ist. Also gilt für den Charakter χ_0 vom ersten Typus oder für χ_0, falls χ vom r-ten Typus ist,

$$\tilde{\varepsilon}_\chi \iota = \tilde{\varepsilon}_\chi \pi^{*f_p} = (\tilde{\varepsilon}_\chi \pi^*)^{f_p};$$

denn es ist $\tilde{\varepsilon}_\chi \pi^* = \pi^* \tilde{\varepsilon}_\chi$ nach (36) und (37). Wenn man in (39) $(p^f)^{-s}$ für u setzt, erhält man ($r_\chi = r_{\chi_i}$, falls χ vom r-ten Typus ist)

$$\begin{aligned}(L_\chi((p^{f_p})^{-s}))^{r_\chi} &= |E - M_l(\tilde{\varepsilon}_\chi \iota) \cdot (p^{f_p})^{-s}| \\ &= |E - M_l((\tilde{\varepsilon}_\chi \pi^*)^{f_p}) \cdot (p^{f_p})^{-s}| \\ &= \prod_{\varrho=1}^{f_p} |E - M_l(\tilde{\varepsilon}_\chi \pi^*) \cdot p^{-s} \cdot \varepsilon^\varrho| \\ &= \prod_{\varrho=1}^{f_p} |E - M_l(\tilde{\varepsilon}_\chi \pi(p)) \cdot p^{-s} \cdot \varepsilon^\varrho|,\end{aligned}$$

wo ε eine primitive f_p-te Einheitswurzel ist.

Aus Teil I erhalten wir nun explizite Ausdrücke für $M^d(\varepsilon_\chi \xi_p)$ und $M^d(\varepsilon_\chi \eta_p)$.

Fall I. *χ ist vom ersten Typus.* Aus (26), (26′) und (42) folgt

$$(43) \qquad |E - M_l(\tilde{\varepsilon}_\chi \pi(p)) \cdot u| = |E_\varkappa - \alpha(p) \cdot \varepsilon_i(p) \cdot u + \varepsilon_i(p^2) \cdot \varepsilon(p) E_\varkappa \cdot pu^2|.$$

Da nun oben $\varphi_p \to \varepsilon_i(p)$ eine Darstellung von $G(Q(\zeta_N)/Q)$ ist, ist $\tilde{\varphi}_p \to \varepsilon_i(p)$ auch eine Darstellung der Gruppe $G(\widetilde{Q(\zeta_N)/Q})$, so daß $\varepsilon_i(p)$ für $i = 1, \ldots, r_\chi$ alle f_p-ten Einheitswurzeln durchläuft. Infolgedessen erhält man, indem man $p^{-s} \cdot \varepsilon^\varrho$ für u setzt und das Produkt über $\varrho = 1, \ldots, f_p$ nimmt,

$$(44) \qquad (L_\chi((p^{f_p})^{-s}))^{r_\chi} = \prod_{\varrho=1}^{f_p} \prod_{i=1}^{r_\chi} |E - \alpha(p)\, \varepsilon_i(p)\, \varepsilon^\varrho p^{-s} + \varepsilon_i(p^2)\, \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}|.$$

Da $(\varepsilon_i(p))$ alle f_p-ten Einheitswurzeln durchläuft, ist $\varepsilon_i(p) = \varepsilon^j$, $j = j(i)$. Die $\varepsilon^{\varrho+j}$ durchlaufen für ein festes j alle f_p-ten Einheitswurzeln ($1 \leqq \varrho \leqq f_p$). Aus (44) folgt dann

$$\begin{aligned}(L_\chi((p^{f_p})^{-s}))^{r_\chi} &= \prod_{\varrho=1}^{f_p} \prod_j |E - \alpha(p)\, \varepsilon^{\varrho+j} p^{-s} + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho+2j}| \\ &= \prod_{\varrho=1}^{f_p} |E - \alpha(p)\, p^{-s} \cdot \varepsilon^\varrho + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}|^{r_\chi}.\end{aligned}$$

Mit anderen Worten: wir erhalten endlich

$$(45) \qquad L_\chi((p^{f_p})^{-s}) = \prod_{\varrho=1}^{f_p} |E - \alpha(p)\, p^{-s} \varepsilon^\varrho + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}|,$$

wo ε eine primitive f_p-te Einheitswurzel und $\varphi_p \to \varepsilon(p)$ ein Charakter von $G(Q(\zeta_N)/Q)$ ist.

Fall II. *χ ist vom r-ten Typus.* Wir betrachten dann, wie in Teil I, den Charakter $\chi_0 = \sum_{i=1}^{r} \chi_i$; nach Annahme ist χ_0 reell. Nun folgen aus (29) und (29)′ explizite Ausdrücke für $M^d(\varepsilon_{\chi_0} \xi_p)$ und $M^d(\varepsilon_{\chi_0} \eta_p)$. Hier sind $\varphi_\lambda \to \varepsilon_i(\lambda)$ Darstellungen der Untergruppe U von $G(Q(\zeta_N)/Q)$.

Man kann diesen Fall auch wie Fall I behandeln, allerdings ist er komplizierter, weil hier $\alpha, \beta, \ldots$ im allgemeinen rechteckige Matrizen sind. Wir interessieren uns jedoch nur für eine Primzahlstufe N, wo die Situation viel einfacher ist, und behandeln diesen Fall im nächsten Teil.

Teil III.

§ 6. Globale Artinsche L-Reihen.

Definition. Mit jedem Charakter χ der Gruppe S definieren wir jetzt eine *globale Artinsche L-Reihe* wie folgt:

$$L(s, \chi, K_N/R_N) = \prod_P{}' L(s, \chi, \widetilde{K}_N/\widetilde{R}_N). \tag{46}$$

Das Produkt läuft über alle Primideale P von $Q(\zeta_N)$, die für $Q(\zeta_N)$ (J) einfach sind.

In diesem Teil betrachten wir den Fall einer *Primzahlstufe* $N = q(\geqq 7)$. Wir beweisen jetzt den

Satz 11 (Hauptsatz). *Für einen einfachen Charakter χ vom ersten Typus von S ist die entsprechende globale Artinsche L-Reihe $L(s, \chi, K_q/R_q)$ eine meromorphe Funktion von s und hat die folgende Form:*

$$L(s, \chi, K_q/R_q) = f(s) \prod_{i=1}^{q-1} |\Phi_i(s)|^{-1}$$

mit einer rationalen Funktion $f(s)$ von p^{-s}. Dabei ist $|\Phi_i(s)|$ die Determinante der Matrix $\Phi_i(s) = \Phi_i(s, \eta_i)$ $(i = 1, \ldots, q-1)$ vom Grade $\varkappa$ (Vielfachheit der Darstellung D mit Charakter χ in M^d), deren Elemente Dirichlet-Reihen sind, die den Spitzenformen vom Grade -2, Stufe q, Teiler 1 und Charakter η_i des Invariantenraumes der Darstellung D zugeordnet sind.

Bevor wir an den Beweis des Satzes gehen, fassen wir kurz einige Resultate von Hecke zusammen, die hier sehr oft benutzt werden. Die Beweise findet man in [5], II.

Aus der Struktur der endlichen Gruppe $S \sim \mathfrak{M}_1(q)$ folgt, daß ihre absolut irreduziblen Darstellungen D_α nur von der Dimension $d = q,\ q+1,\ q-1,\ \frac{q+1}{2},\ \frac{q-1}{2}$ oder gleich der Identitätsdarstellung sein können. Da wir uns mit den Formen vom Grade -2 beschäftigen, haben die Identitätsdarstellung und im Falle $q \equiv 3 \pmod 4$ die Darstellungen der Dimension $\frac{q+1}{2}$ und im Falle $q \equiv 1 \pmod 4$ diejenigen der Dimension $\frac{q-1}{2}$ die Vielfachheit 0 in M^d.

Aus der Charakterentafel und der Struktur des Zentrums der Gruppenalgebra $R(k)$ von S erhalten wir nach Hecke [5], II:

Satz 12. *Die irreduziblen Darstellungen vom Grade q, $q+1$, $q-1$ sind vom ersten Typus, und die irreduziblen Darstellungen der Grade $\frac{q+1}{2}$, $\frac{q-1}{2}$ (je zwei) sind vom zweiten Typus.*

Ferner sind die Charaktere χ aller Darstellungen vom ersten Typus reell und $\chi_0 = \chi + \bar{\chi}$, die Summe der beiden inäquivalenten Darstellungen gleichen Grades vom zweiten Typus, ist auch reell. Deshalb können wir die Betrachtungen von Teil II auf diese Darstellungen und Charaktere anwenden.

Jeder Invariantenraum G zu einer irreduziblen Darstellung D läßt sich in die direkte Summe $G = E_1 + E_q$ von 2 Formen-Scharen vom Teiler 1 bzw. q zerlegen. Diese Unterräume bleiben für Substitutionen aus der Untergruppe $\mathfrak{M}_0(q) \sim \Gamma_0(q)/\Gamma_1(q)$ von $\mathfrak{M}_1(q)$ invariant. E_1 enthält nur irreduzible Darstellungen $U_{\frac{q-1}{2}}$ vom Grade $\frac{q-1}{2}$ von $\mathfrak{M}_0(q)$, und E_q nur irreduzible Darstellungen U_1 vom Grade 1. Diese irreduziblen Darstellungen U verteilen sich auf diejenigen von $\mathfrak{M}_1(q)$ wie folgt ([5], II):

Satz 13. 1) $d = q - 1$: *jede* G_{q-1} *enthält zwei inäquivalente* $U_{\frac{q-1}{2}}$.

2) $d = q$: *jede* G_q *enthält die Identitätsdarstellung von* $\mathfrak{M}_0(q)$ *und ferner zwei inäquivalente* $U_{\frac{q-1}{2}}$.

3) $d = q + 1$: *jede* G_{q+1} *enthält zwei konjugiert komplexe Darstellungen* U_1 *und zwei inäquivalente* $U_{\frac{q-1}{2}}$. *Verschiedene* G_{q+1} *enthalten verschiedene* U_1.

4) $d = \frac{q-1}{2}$; *beide* $G_{\frac{q-1}{2}}$ *enthalten je eine* $U_{\frac{q-1}{2}}$, *aber nicht dieselbe.*

5) $d = \frac{q+1}{2}$: *beide* $G_{\frac{q+1}{2}}$ *enthalten eine reelle* U_1 *(verschieden von der Identität) und eine* $U_{\frac{q-1}{2}}$, *aber nicht dieselbe.*

Jetzt betrachten wir die irreduziblen Darstellungen vom ersten Typus, die nach Satz 12 von der Dimension $q - 1$, q, $q + 1$ sind.

Jeder irreduziblen Darstellung D vom ersten Typus haben wir in Teil II die Matrix $A_n = (\varepsilon_i(n)\,\delta_{ik})$ zugeordnet, wo $\varphi_n \to \varepsilon_i(n)$ Darstellungen von $G(Q(\zeta_N)/Q)$ sind, und entsprechend gilt für die Matrix $M(R_n) = (\varepsilon_i(n^2) \cdot \varepsilon(n)\,\delta_{ik})$. Dann folgt aus den Sätzen 54, 55, 56 von Hecke ([5], II), daß für die Matrix $\Phi_i(s) = \Phi_i(s, \eta_i)$ $(i = 1, \ldots, q - 1)$ vom Grade $\varkappa$, deren Elemente (wie in Satz 13) Dirichlet-Reihen sind, die Eulerproduktentwicklung gilt:

$$\Phi_i(s) = \prod_{\substack{p \\ (p \neq q)}} [E - \alpha(p)\, p^{-s} \varepsilon_i(p) + \varepsilon_i(p^2)\, \varepsilon(p)\, p^{1-2s} E]^{-1}. \tag{47}$$

ε_i $(i = 1, \ldots, q - 1)$ läuft über alle Charaktere von $G(Q(\zeta_q)/Q)$. $\alpha(p)$ und $\varepsilon(p)$ hängen natürlich von der Darstellung D ab. Für das Produkt von (47) über alle i haben wir

$$\prod_{i=1}^{q-1} \Phi_i(s) = \prod_{\varepsilon_i} \prod_{\substack{p \\ (p \neq q)}} [E - \alpha(p)\, \varepsilon_i(p) p^{-s} + \varepsilon_i(p^2)\, \varepsilon(p)\, E p^{1-2s}]^{-1}.$$

Da f_p der Restklassengrad von P in $Q(\zeta_q)$ ist, sind $\varepsilon_i(p)$ f_p-te Einheitswurzeln, und in dem Produkt kommt jedes $\varepsilon_i(p)$ genau g_p-mal vor, wo g_p folgendermaßen erklärt ist: p zerlegt sich in $Q(\zeta_q)$ in g_p Faktoren: $p = P_1, \ldots P_{g_p}$, mit $N(P_i) = p^{f_p}$ (alle Primzahlen $p \neq q$ sind in $Q(\zeta_q)$ unverzweigt). Daraus folgt

$$\prod_{i=1}^{q-1} \Phi_i(s) = \prod_{\substack{p \\ (p \neq q)}} \prod_{\varrho=1}^{f_p} [E - \alpha(p)\, \varepsilon^\varrho p^{-s} + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}]^{-g_p}, \tag{48}$$

wo ε eine primitive f_p-te Einheitswurzel ist.

Nach dieser Vorbereitung sind wir in der Lage, den Hauptsatz zu beweisen. Aus (46) haben wir

$$\begin{aligned} L(s, \chi, K_q/R_q) &= \prod_P{}' L(s, \chi, \tilde{K}_q/\tilde{R}_q) \\ &= \prod_p{}' \prod_{P|p} L(s, \chi, \tilde{K}_q/\tilde{R}_q). \end{aligned}$$

Für ein zulässiges P gilt nach (45) für einen Charakter vom ersten Typus

$$L(s, \chi, \tilde{K}_q/\tilde{R}_q) = \prod_{\varrho=1}^{f_p} \left| E - \alpha(p)\, p^{-s} \varepsilon^\varrho + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho} \right|.$$

Da nun die rechte Seite nur von p abhängig ist, so ist $L(s, \chi, \tilde{K}_q/\tilde{R}_q)$ für alle Primideale P von $Q(\zeta_q)$, die in p aufgehen, die gleiche Funktion, somit:

$$\prod_{P|p} L(s, \chi, \tilde{K}_q/\tilde{R}_q) = \prod_{\varrho=1}^{f_p} \left| E - \alpha(p)\, p^{-s} \varepsilon^\varrho + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho} \right|^{g_p}.$$

Durch Vergleich mit (48) erhalten wir endlich

$$(49)\qquad \begin{aligned} L(s,\chi,K_q/R_q) &= \prod_p{}' \prod_{P\mid p} L(s,\chi,\widetilde{K}_q/\widetilde{R}_q) \\ &= \prod_p{}' \,|\, E-\alpha(p)\,p^{-s}\varepsilon^{\varrho}+\varepsilon(p)\,Ep^{1-2s}\varepsilon^{2\varrho}\,|^{g_p} \\ &= \prod_{i=1}^{q-1} |\,\Phi_i(s)\,|^{-1}\cdot f(s), \end{aligned}$$

wo $|\,\Phi_i(s)\,|$ die Determinante von $\Phi_i(s)$ und $f(s)$ ein Produkt von endlich vielen rationalen Funktionen von p^{-s} (p unzulässig) ist.

Wir betrachten jetzt die irreduziblen Darstellungen vom zweiten Typus. Wenn D_1, D_2 die zwei inäquivalenten irreduziblen Darstellungen vom zweiten Typus sind, so gilt $D_2 = \bar{D}_1$. Der Charakter $\chi_0 = \chi_1 + \chi_2 = \chi_1 + \bar{\chi}_1$ ist reell, so daß die Resultate des Teils II hier angewandt werden können.

Wir nehmen zuerst den Fall des Grades $\frac{q-1}{2}$. In diesem Fall muß $q \equiv 3 \pmod 4$ sein. Ferner folgt aus Satz 12, daß die Darstellung D_1, eingeschränkt auf $\mathfrak{M}_0(q)$, eine irreduzible Darstellung des Grades $\frac{q-1}{2}$ enthält. Das bedeutet dann, daß dieser Invariantenraum nur Formen von Teiler 1 enthält.

Wenn man den Automorphismus $\zeta_q \to \zeta_q^{-1} = \bar{\zeta}_q$ von $Q(\zeta_q)/Q$ mit φ bezeichnet, gilt folgendes:

Entweder a) $\varphi_p \in U$ oder b) $\varphi_p\varphi \in U$, wo U die Untergruppe (φ_λ) von $G(Q(\zeta_q)/Q)$ mit der Eigenschaft $D_1^{\varphi_\lambda} \sim D_1$ ist. Dieses gilt, da U in der Gruppe $G(Q(\zeta_q)/Q)$ den Index 2 hat, wo U und $U\varphi$ die Nebenklassen sind.

In jedem Fall folgt aus (29) und (29′)

$$M^d(\varepsilon_{\chi_0}\xi_p) \sim \begin{pmatrix} \gamma(p)\,\varepsilon_1(p) & 0 & \cdot & \cdot & 0 \\ 0 & & & & \cdot \\ \cdot & & \cdot & & \cdot \\ \cdot & & & \cdot & \cdot \\ \cdot & & & \cdot & 0 \\ 0 & \cdot & \cdot & 0 & \gamma(p)\,\varepsilon_{r_\chi}(p) \end{pmatrix}$$

mit einer $(\varkappa,\varkappa)$-Matrix $\gamma(p)$ $(\varkappa = \varkappa_1 + \varkappa_2)$ und $A_p = (\varepsilon_i(p)\,\delta_{ik})$. ε_i sind die $\frac{q-1}{2}$ Charaktere der Gruppe U und $\varepsilon_i(p) = \varepsilon_i(\varphi_p)$ oder $\varepsilon_i(\varphi_p\varphi)$ je nachdem, ob $\varphi_p \in U$ oder $\varphi_p\varphi \in U$ ist. Entsprechend gilt

$$M^d(\varepsilon_{\chi_0}\eta_p) \sim \begin{pmatrix} \varepsilon_1^2(p)\cdot\varepsilon(p)\cdot E & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & & & & & \cdot \\ \cdot & & \cdot & & & \cdot \\ \cdot & & & \cdot & & \cdot \\ \cdot & & & & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & \varepsilon_{r_\chi}^2(p)\cdot\varepsilon(p)E \end{pmatrix}$$

mit einem Charakter ε der Gruppe U und $\varepsilon(p) = \varepsilon(\varphi_p)$ oder $\varepsilon(\varphi_p\varphi)$ je nachdem, ob $\varphi_p \in U$ oder $\varphi_p\varphi \in U$ ist.

Nun folgt aus (39)′

$$\begin{aligned} L(s,\chi_0,\widetilde{K}_q/\widetilde{R}_q)^{\frac{q-1}{2}} &= |\,E - M_l(\widetilde{\varepsilon}_{\chi_0 l})\,(p^{f_p})^{-s}\,| \\ &= \prod_{\varrho=1}^{f_p} |\,E - M_l(\widetilde{\varepsilon}_{\chi_0}\pi(p))\,p^{-s}\cdot\varepsilon^{\varrho}\,| \end{aligned}$$

mit einer primitiven f_p-ten Einheitswurzel ε. Es ist aber

$$\begin{aligned}|E - M_l(\tilde{\varepsilon}_{\chi_0}\pi(p))\,u\,|^2 &= |E - M_l(\tilde{\varepsilon}_{\chi_0}\pi(p))\,u\,|\cdot|E - M_l(\tilde{\varepsilon}_{\chi_0}\pi(p)')\,u\,| \\ &= |E - M_l(\tilde{\varepsilon}_{\chi_0}\tilde{\xi}_p)\,u + M_l(\tilde{\varepsilon}_{\chi_0}\tilde{\eta}_p)\,pu^2\,| \\ &= |E - M_l(\varepsilon_{\chi_0}\xi_p)\,u + M_l(\varepsilon_{\chi_0}\eta_p)\,pu^2\,| \\ &= |E - M^d(\varepsilon_{\chi_0}\xi_p)\,u + M^d(\varepsilon_{\chi_0}\eta_p)\,pu^2\,| \\ &\qquad\cdot|E - \overline{M^d(\varepsilon_{\chi_0}\xi_p)}\,u + \overline{M^d(\varepsilon_{\chi_0}\eta_p)}\,pu^2\,|.\end{aligned}$$

Also haben wir

$$\begin{aligned}(L(s,\chi_0,\tilde{K}_q/\tilde{R}_q))^{q-1} = \prod_{\varrho=1}^{f_p} &|E - M^d(\varepsilon_{\chi_0}\xi_p)\,p^{-s}\varepsilon^\varrho + M^d(\varepsilon_{\chi_0}\eta_p)\,p^{1-2s}\varepsilon^{2\varrho}\,| \\ &\cdot|E - \overline{M^d(\varepsilon_{\chi_0}\xi_p)}\,p^{-s}\varepsilon^\varrho + \overline{M^d(\varepsilon_{\chi_0}\eta_p)}\,p^{1-2s}\varepsilon^{2\varrho}\,|.\end{aligned}$$

Wenn man die expliziten Ausdrücke für $M^d(\varepsilon_{\chi_0}\xi_p)$ und $M^d(\varepsilon_{\chi_0}\eta_p)$ einsetzt, erhält man

$$\begin{aligned}L(s,\chi_0,\tilde{K}_q/\tilde{R}_q)^{q-1} = \prod_{\varrho=1}^{f_p}\Bigg[\prod_{i=1}^{\frac{q-1}{2}} &|E - \gamma(p)\,p^{-s}\varepsilon_i(p)\,\varepsilon^\varrho + \varepsilon(p)\,Ep^{1-2s}\varepsilon^{2\varrho}\varepsilon_i(p^2)\,| \\ &\cdot|E - \overline{\gamma(p)}\,p^{-s}\overline{\varepsilon_i(p)}\,\varepsilon^\varrho + \overline{\varepsilon(p)}\,Ep^{1-2s}\varepsilon^{2\varrho}\overline{\varepsilon_i(p^2)}\,|\Bigg].\end{aligned}$$

Da ε_i Charaktere der Gruppe U sind, sind $\varepsilon_i(p)$ f'_p-te Einheitswurzeln, wo f'_p den Restklassengrad des Unterkörpers von $Q(\zeta_q)$ bedeutet, der durch U definiert wird. f'_p ist ein Teiler von f_p, so daß $\varepsilon_i(p) = \varepsilon^j$, $j = j(i)$ ist. Für ein festes j liefert die Menge $(\varepsilon^{\varrho+j})$ ein volles System f_p-ter Einheitswurzeln, so daß

$$\begin{aligned}L(s,\chi_0,\tilde{K}_q/\tilde{R}_q)^2 = \prod_{\varrho=1}^{f_p}[\,&|E - \gamma(p)\,p^{-s}\cdot\varepsilon^\varrho + \varepsilon(p)\,Ep^{1-2s}\varepsilon^{2\varrho}\,| \\ &\cdot|E - \overline{\gamma(p)}\,p^{-s}\cdot\varepsilon^\varrho + \overline{\varepsilon(p)}\,Ep^{1-2s}\varepsilon^{2\varrho}\,|]\end{aligned}$$

gilt.

Da dieser Ausdruck auf der rechten Seite nur von p abhängt, ist er für alle Primideale P von $Q(\zeta_q)$, die in p aufgehen, gleich. Somit haben wir

$$\begin{aligned}\prod_{P|p} L(s,\chi_0,\tilde{K}_q/\tilde{R}_q)^2 = \prod_{\varrho=1}^{f_p}[\,&|E - \gamma(p)\,p^{-s}\varepsilon^\varrho + \varepsilon(p)\,Ep^{1-2s}\varepsilon^{2\varrho}\,| \\ &\cdot|E - \overline{\gamma(p)}\,p^{-s}\cdot\varepsilon^\varrho + \overline{\varepsilon(p)}\,Ep^{1-2s}\varepsilon^{2\varrho}\,|]^{g_p}.\end{aligned}$$

Für die globale Artinsche L-Reihe gilt dann

$$\begin{aligned}L(s,\chi_0,K_q/R_q)^2 &= \prod_P{}' L(s,\chi_0,\tilde{K}_q/\tilde{R}_q)^2 \\ &= \prod_p{}' \prod_{p|P} L(s,\chi_0,\tilde{K}_q/\tilde{R}_q)^2 \\ &= \prod_p{}' \prod_{\varrho=1}^{f_p}[\,|E - \gamma(p)\,p^{-s}\cdot\varepsilon^\varrho + \varepsilon(p)\,Ep^{1-2s}\varepsilon^{2\varrho}\,| \\ &\qquad\cdot|E - \overline{\gamma(p)}\,p^{-s}\cdot\varepsilon^\varrho + \overline{\varepsilon(p)}\,Ep^{1-2s}\varepsilon^{2\varrho}\,|]^{g_p}.\end{aligned}$$

Für den Grad $\frac{q+1}{2}$ erhält man ein ähnliches Resultat, indem man die Darstellungen von ξ_p, η_p in einem Unterraum nimmt, der im Invariantenraum aus den Formen vom Teiler 1 besteht.

Bemerkung: In den beiden obigen Fällen vom zweiten Typus scheint es zwischen den globalen Artinschen L-Reihen und den Eulerproduktentwicklungen der Dirichletreihen-Matrizen die diesem Raum zugeordnet sind, keinen direkten Zusammenhang (wie im Fall des ersten Typus) zu geben.

Korollar zum Hauptsatz: Wir können jetzt einige Folgerungen aus dem Hauptsatz ziehen.

Wir betrachten die irreduzible Darstellung des Grades q. Wenn sie auf die Untergruppe $\mathfrak{M}_0(q)$ $(\sim \Gamma_0(q)/\Gamma_1(q))$ eingeschränkt wird, enthält sie die Identitätsdarstellung, und umgekehrt ist die Identitätsdarstellung von $\mathfrak{M}_0(q)$ nur in dieser Darstellung enthalten (Satz 12).

Wenn also T_q den entsprechenden Unterkörper von K_q bedeutet, folgt aus der Artinschen Theorie für einen Charakter ψ von $\mathfrak{M}_0(q)$, daß

$$L(s, \psi, \widetilde{K}_q/\widetilde{T}_q) = L(s, \chi_\psi, \widetilde{K}_q/\widetilde{R}_q)$$

gilt, wo χ_ψ der Charakter der imprimitiven Darstellung ist, der durch ψ auf $\mathfrak{M}_1(q)$ induziert wird. Für $\psi = 1$ gilt sogar

$$L(s, 1, \widetilde{K}_q/\widetilde{T}_q) = \zeta(s, \widetilde{T}_q),$$

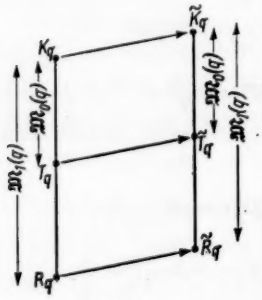


Fig. 4

und χ_1 ist der Charakter der induzierten Darstellung von 1 auf $\mathfrak{M}_1(q)$. Diese imprimitive Darstellung des Grades $q+1$ (Index von $\mathfrak{M}_0(q)$ in $\mathfrak{M}_1(q)$) enthält die irreduzible Darstellung des Grades q und die Identitätsdarstellung des Grades 1. Infolgedessen gilt

$$\begin{aligned}\zeta(s, \widetilde{T}_q) &= L(s, 1, \widetilde{K}_q/\widetilde{T}_q)\\ &= L(s, \chi_1, \widetilde{K}_q/\widetilde{R}_q)\\ &= L(s, 1, \widetilde{K}_q/\widetilde{R}_q) \cdot L(s, \chi_q, \widetilde{K}_q/\widetilde{R}_q)\\ &= \zeta(s, \widetilde{R}_q) \cdot L(s, \chi_q, \widetilde{K}_q/\widetilde{R}_q).\end{aligned}$$

Nun bilden wir das Produkt über alle zulässigen Primideale P auf beiden Seiten; dann ergibt sich

$$\zeta(s, T_q) = f_1(s) \cdot \zeta(s, R_q) \cdot \prod_{i=1}^{q-1} |\Phi_i(s)|^{-1} \tag{50}$$

mit einer rationalen Funktion $f_1(s)$ von p^{-s} und $\Phi_i(s)$ wie im Hauptsatz.

Folglich ist $\zeta(s, T_q)$ wieder eine meromorphe Funktion von s; denn $\zeta(s, R_q)$ ist ein Produkt von Dedekindschen Zetafunktionen von $Q(\zeta_q)$, da R_q ein rationaler Funktionenkörper über $Q(\zeta_q)$ ist.

Teil IV.

§ 7. Allgemeine Struktur globaler Artinscher L-Reihen.

Im vorigen Teil definierten wir eine globale Artinsche L-Reihe, die jedem Charakter χ der Gruppe S zugeordnet ist und bewiesen, daß sie für bestimmte Charaktere (und für Primzahlstufe) eine meromorphe Funktion von s ist.

Wir betrachten in diesem Teil die allgemeine Situation einer Galois-Überlagerung (mit Galoisgruppe G) einer gegebenen Kurve Γ über einem algebraischen Zahlkörper k und suchen Bedingungen dafür, daß die globale Artinsche L-Reihe bezüglich eines Charakters χ von G sich als ein Produkt von L-Reihen mit Größencharakteren in k schreiben läßt. Es folgt dann, daß diese Reihen meromorphe Funktionen sind. Dazu benutzen wir, etwas modifiziert, die Methode von Taniyama. Wir reduzieren dieses Problem auf das Taniyamasche Problem, um seine Resultate anwenden zu können [11].

Sei Γ eine nicht-singuläre vollständige Kurve über einem algebraischen Zahlkörper k und sei $K = k(u)$ mit einem allgemeinen Punkt u von Γ bezüglich k. Wir bezeichnen mit K_0 einen solchen Unterkörper von K, daß K/K_0 eine Galoiserweiterung mit Galoisgruppe G ist. Ferner nehmen wir an, daß k auch der Konstantenkörper von K_0 ist. Wir bezeichnen mit J eine Jacobische Mannigfaltigkeit von Γ über k und betrachten diejenigen Primideale $\mathfrak{p}$ von k, für welche J keinen Defekt hat. Wir können dann die reduzierte Kurve $\tilde{\Gamma}$ und deren Jacobische Mannigfaltigkeit $\tilde{J}$ bilden. $\tilde{K}$ ist dann eine Galoissche Erweiterung von $\tilde{K}_0$, und wir erhalten mit jedem Charakter χ von G die entsprechende Artinsche L-Reihe $L(s, \chi, \tilde{K}/\tilde{K}_0)$ und damit auch die globale Artinsche L-Reihe wie im Teil III:

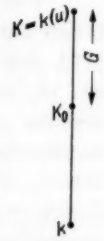


Fig. 5

$$L(s, \chi, K/K_0) = \prod_{\mathfrak{p}}{}' L(s, \chi, \tilde{K}/\tilde{K}_0),$$

wo das Produkt über alle zulässigen Primideale $\mathfrak{p}$ von k läuft.

Das Problem ist jetzt, zu untersuchen, unter welchen Bedingungen $L(s, \chi, K/K_0)$ ein Produkt von L-Reihen mit Größencharakteren in k ist.

Sei ε_χ das Idempotent, das dem Charakter χ zugeordnet ist:

$$\varepsilon_\chi = \frac{r_\chi}{g_0} \sum_{\alpha \in G} \chi(\alpha^{-1}) \cdot \xi_\alpha;$$

dabei ist g_0 die Ordnung von G, ξ_α die Korrespondenzklasse (oder der Endomorphismus von J) der Korrespondenz $\alpha \in G$ und $r_\chi = \chi(1)$. ε_χ ist im allgemeinen ein Element von $\mathfrak{A}_0(J) \otimes k_1$ mit einer Erweiterung k_1 von k.

Sei $\mathfrak{p}$ ein für K reguläres Primideal von k. Wir bezeichnen mit $\mathfrak{B}$ einen Primteiler von $\mathfrak{p}$ in $\bar{k}$ und mit $\sigma_{\mathfrak{B}}$, einen $\mathfrak{B}$ zugeordneten Frobeniusschen Automorphismus in $G(\bar{k}/k)$. Nach Taniyama ([11], S. 359) hat $G(\bar{k}/k)$ eine l-adische Darstellung M_l in J, und durch Reduktion modulo $\mathfrak{p}$ geht $M_l(\sigma_{\mathfrak{B}})$ in $M_l(\pi_{\mathfrak{p}})$ über ($\pi_{\mathfrak{p}}$ der Frobeniussche Automorphismus von J, der $\mathfrak{p}$ zugeordnet ist).

Nun impliziert $\varepsilon_\chi \pi_{\mathfrak{p}} = \pi_{\mathfrak{p}} \tilde{\varepsilon}_\chi$ die Identität $M_l(\tilde{\varepsilon}_\chi \pi_{\mathfrak{p}}) = M_l(\pi_{\mathfrak{p}} \tilde{\varepsilon}_\chi)$, und das bedeutet weiter, daß $M_l(\varepsilon_\chi \sigma_{\mathfrak{B}}) = M_l(\sigma_{\mathfrak{B}} \varepsilon_\chi))$ ist. Da $(\sigma_{\mathfrak{B}})$ in $G(\bar{k}/k)$ überall dicht liegt, folgt wegen der Stetigkeit, daß $M_l(\varepsilon_\chi)$ mit $M_l(\sigma)$ für alle $\sigma \in G(\bar{k}/k)$ vertauschbar ist. Infolgedessen bilden die Abbildungen $\sigma \to M_l(\varepsilon_\chi \sigma)$ ein System von l-adischen Darstellungen der Gruppe $G(\bar{k}/k)$.

Jetzt zeigen wir: Erfüllt das System $\{M^*_{l,\chi}(\sigma) = M_l(\varepsilon_\chi \sigma)\}$ von Darstellungen von $G(\bar{k}/k)$ eine Reihe von noch anzugebenden Bedingungen, dann ist die entsprechende globale Artinsche L-Reihe $L(s, \chi, K/K_0)$ ein Produkt von L-Reihen mit Größencharakteren in k *vom Typ* (A_0). Diese Charaktere sind folgendermaßen definiert:

Ein *Größencharakter* im Sinne Heckes läßt sich als ein *Idèleklassencharakter* von k betrachten, d. h. als ein Charakter der Idèleklassengruppe C_k von k. Ein Charakter ϱ von C_k ist vom *Typ* (A_0) im Sinne Weils [15], [11], wenn er die folgenden Bedingungen erfüllt: Sei $\mathfrak{f}$ der Führer von ϱ. Dann gibt es stets einen Charakter X von k^* (multiplikative Gruppe von k) mit $X(\alpha) = \tilde{\varrho}((\alpha))$ für jedes $\alpha \in k^*$ mit $\alpha \equiv 1 \pmod{\mathfrak{f}}$ und das Hauptideal (α) von α ($\tilde{\varrho}$ ist der von ϱ induzierte Charakter auf der Gruppe $G(\mathfrak{f})$, die aus den zu $\mathfrak{f}$ primen Idealen besteht). ϱ ist *vom Typ* (A_0), wenn das entsprechende X die folgende Form annimmt:

$$X(\alpha) = \pm \prod_{\sigma \in H(k)} \sigma\alpha^{n(\sigma)}$$

wobei $H(k)$ die Gesamtheit aller Isomorphismen von k/Q bedeutet; $n(\sigma)$ sind ganze Zahlen, und das Vorzeichen $\pm$ ist von α abhängig.

Für ein ϱ vom Typ (A_0) liegen sämtliche Werte $\varrho(\mathfrak{a})$ für $\mathfrak{a} \in G(\mathfrak{f})$ in einem endlichen algebraischen Zahlkörper L. Sei $\mathfrak{l}$ ein Primideal in L. Dann folgt nach Taniyama [11], daß ϱ ein System von Darstellungen $(\varrho_{\mathfrak{l}})$ von C_k in die Einheitengruppe $U_{\mathfrak{l}}$ von $L_{\mathfrak{l}}^*$ ist. ($L_{\mathfrak{l}}$ ist die vollständige Hülle von L bezüglich der $\mathfrak{l}$-adischen Bewertung.) Die Darstellung $\varrho_{\mathfrak{l}}$ induziert ferner eine Darstellung $\varrho_{\mathfrak{l}}^*$ von $C_k' = C_k/D_k$ (D_k bedeutet die zusammenhängende Komponente der Identität in C_k). Es folgt dann aus der Klassenkörpertheorie, daß C_k' kanonisch isomorph mit der Galoisgruppe G_k der maximalen abelschen Erweiterung A_k von k ist. So haben wir ein System von Darstellungen $(\varrho_{\mathfrak{l}}^*)$ von G_k, die ϱ zugeordnet sind. Das System $(\varrho_{\mathfrak{l}}^*)$ charakterisiert vollständig den Charakter ϱ nach Satz 1 von Taniyama [11]. (Es sei hier bemerkenswert, daß $\varrho_{\mathfrak{l}}^*(\sigma_{\mathfrak{p}}) = \varrho_{\mathfrak{l}}(\iota_{\mathfrak{p}}\pi_{\mathfrak{p}}) = \tilde{\varrho}(\mathfrak{p})$ für jedes $\mathfrak{p} \in G(\mathfrak{f}\mathfrak{l})$ gilt, wo $\sigma_{\mathfrak{p}}$ der Frobeniussche Automorphismus von $\mathfrak{p}$ in G_k, $\pi_{\mathfrak{p}}$ ein $\mathfrak{p}$-Primelement in $k_{\mathfrak{p}}^*$ und $\iota_{\mathfrak{p}}$ die Einbettung ist.

Wir nehmen jetzt ein System von Darstellungen $\{M_{l,\chi}^*(\sigma) = M_l(\varepsilon_\chi \sigma)\}$ der Gruppe $G(\bar{k}/k)$ her und zeigen, daß es, wenn nachstehende Bedingungen erfüllt sind, zu einem System von eindimensionalen Darstellungen $(\psi_{\mathfrak{l}}^*)$ von G_k führt, das die Bedingungen $(\mathrm{CA}_{\mathrm{I}})$ bis $(\mathrm{CA}_{\mathrm{IV}})$ von Taniyama ([11], S. 338) erfüllt.

Bezeichnen wir mit $\mathfrak{B}$ einen der Primteiler von $\mathfrak{p}$ in $\bar{k}$ und mit $\bar{G}(\mathfrak{a})$ die Gesamtheit aller Primteiler $\mathfrak{B}$ von $\mathfrak{p}$ in $\bar{k}$ für alle $\mathfrak{p} \in G(\mathfrak{a})$ für ein ganzes Ideal $\mathfrak{a}$ von k. Dann sind es die folgenden Bedingungen (vergleiche [11], S. 350):

1) Es gibt ein ganzes Ideal $\mathfrak{m}$ in k mit der Eigenschaft, daß $M_{1,\chi}^*(\sigma_{\mathfrak{B}})$ von der Wahl von $\sigma_{\mathfrak{B}}$ für jedes $\mathfrak{B} \in \bar{G}(\mathfrak{m}l)$ unabhängig ist.

Wir bezeichnen mit k_1' den Körper aller Matrizen λE mit $\lambda \in k_1$ und der Einheitsmatrix E.

2) Die Matrizen $\{M_{l,\chi}^*(\sigma_{\mathfrak{B}})\}$ für alle $\mathfrak{B} \in \bar{G}(\mathfrak{m}l)$ erzeugen über k_1' eine kommutative halbeinfache Algebra $\mathfrak{A}_{l,\chi}$ von endlichem Rang über k_1.

Ferner bestimmt die Korrespondenz $M_{l,\chi}^*(\sigma_{\mathfrak{B}}) \rightleftarrows M_{q,\chi}^*(\sigma_{\mathfrak{B}})$ für alle $\mathfrak{B} \in \bar{G}(\mathfrak{m}lq)$ einen Isomorphismus von $\mathfrak{A}_{l,\chi}$ auf $\mathfrak{A}_{q,\chi}$ für alle Primzahlpaare (l, q).

3) Die charakteristische Gleichung von $M_{l,\chi}^*(\sigma_{\mathfrak{B}})$ hat Koeffizienten in k_1 und ist von l unabhängig für alle l mit $\mathfrak{B} \in \bar{G}(\mathfrak{m}l)$.

Seien $\tilde{\omega}_1(\mathfrak{p}), \ldots, \tilde{\omega}_{d_\chi}(\mathfrak{p})$ die sämtlichen Wurzeln dieses Polynoms (mit den richtigen Vielfachheiten). Sie hängen nur von $\mathfrak{p}$ ab und sind von $\mathfrak{B}$ unabhängig.

4) Es gilt $|\tilde{\omega}_i(\mathfrak{p})| = N\mathfrak{p}^\lambda$ für alle $\mathfrak{p} \in G(\mathfrak{m})$, wo λ eine halbganze von $\mathfrak{p}$ und von i unabhängige Zahl ist.

5) Es gibt eine solche natürliche Zahl n_0, daß $\tilde{\omega}_i(\mathfrak{p}) \cdot N\mathfrak{p}^{n_0}$ für alle $\mathfrak{p} \in G(\mathfrak{m})$ und für alle i algebraische ganze Zahlen sind.

Da $(\sigma_{\mathfrak{B}})$ in $G(\bar{k}/k)$ überall dicht liegt, schließen wir aus 2), daß die Bildmenge $\{M_{l,\chi}^*(G(\bar{k}/k))\}$ eine abelsche Gruppe sein muß. Mit anderen Worten: Das System $\{M_{l,\chi}^*\}$ läßt sich als ein System von Darstellungen der abelschen Gruppe $G_k = G(A_k/k)$ betrachten, und deshalb kann $\sigma_{\mathfrak{p}}$ statt $\sigma_{\mathfrak{B}}$ geschrieben werden. Da nun $\mathfrak{A}_{l,\chi}$ eine kommutative halbeinfache Algebra ist, gilt $\mathfrak{A}_{l,\chi} = \sum_i L_{i,\chi} \cdot \varepsilon_i$ mit Idempotenten ε_i und endlichen Erweiterungen $L_{i,\chi}$ von k_1. Ohne Beschränkung der Allgemeinheit dürfen wir jetzt annehmen, daß $\mathfrak{A}_{l,\chi}$ ein algebraischer Zahlkörper L_χ ist und $L_\chi \cong \{M_{l,\chi}^*(\sigma_{\mathfrak{B}})\}$ mit einem Isomorphismus μ_l gilt. Wir wählen diesen Isomorphismen μ_l derart, daß

$$\mu_l(M_{l,\chi}^*(\sigma_{\mathfrak{p}})) = \mu_q(M_{q,\chi}^*(\sigma_{\mathfrak{p}}))$$

für alle $\mathfrak{p} \in G(\mathfrak{m}lq)$ und für alle Primzahlpaare (l, q) gilt. Der gemeinsame Wert soll mit $\tilde{\psi}(\mathfrak{p})$ bezeichnet werden.

Nun können alle $M^*_{l,\chi}(\sigma)$ in $\bar{Q}_l$ folgendermaßen auf Diagonalform gebracht werden:

$$M^*_{l,\chi}(\sigma) = \begin{pmatrix} \psi^{**}_{l,1}(\sigma) & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & \cdot & & & & \cdot \\ \cdot & & \cdot & & & \cdot \\ \cdot & & & \cdot & & \cdot \\ \cdot & & & & & 0 \\ 0 & \cdot & \cdot & \cdot & 0 & \psi^{**}_{l,d}(\sigma) \end{pmatrix}.$$

Für jedes i liefert der Isomorphismus $\psi(\mathfrak{p}) \to \psi^{**}_{l,i}(\sigma_\mathfrak{p})$ für $\mathfrak{p} \in G(\mathfrak{m}l)$ einen Isomorphismus $\mu_{l,i}: L_\chi \to \bar{Q}_l$, der einen Primdivisor $\mathfrak{l}_i$ von l in L_χ definiert. Wenn man $\psi^*_{\mathfrak{l}_i} = \mu^{-1}_{l,i} \cdot \psi^{**}_{l,i}$ setzt, dann ist $\psi^*_\mathfrak{l}$ eine Darstellung von G_k in $L^*_{\chi,\mathfrak{l}_i}$. Das System $(\psi^*_\mathfrak{l})$ von Darstellungen von G_k erfüllt die Bedingungen $(\mathrm{CA_I})$ bis $(\mathrm{CA_{IV}})$ von Taniyama, wie man sofort sieht. Daraus folgt, daß sie aus einem Charakter ϱ von C_k vom Typ (A_0) stammen.

Bisher war die Darstellung $\tilde{\psi}(\mathfrak{p}) \to M^*_{l,\chi}(\sigma_\mathfrak{p})$ treu, und die reguläre Darstellung von L_χ ist mit einer gewissen Vielfachheit darin enthalten, so daß die verschiedenen charakteristischen Wurzeln $\tilde{\omega}_i(\mathfrak{p})$ von $M^{**}_{l,\chi}(\sigma_\mathfrak{p})$ alle miteinander konjugiert sind. Wenn wir mit τ_i die verschiedenen Automorphismen von L_χ bezeichnen, ist ϱ^{τ_i} ein Charakter von C_k vom Typ (A_0) mit der Eigenschaft $\widetilde{\varrho^{\tau_i}}(\mathfrak{p}) = (\tilde{\varrho}(\mathfrak{p}))^{\tau_i} = (\tilde{\psi}(\mathfrak{p}))^{\tau_i} = \tilde{\omega}_i(\mathfrak{p})$. Indem wir für alle Komponenten $L_{i,\chi}$ von $\mathfrak{A}_{l,\chi}$ dieselben Überlegungen anstellen, erkennen wir, daß dem System der Darstellungen $\{M^*_{l,\chi}(\sigma)\}$ eine Menge von Charakteren (ϱ_i) vom Typ (A_0) zugeordnet ist, und zwar so, daß $\tilde{\varrho}_i(\mathfrak{p}) = \tilde{\omega}_i(\mathfrak{p})$ für $i = 1, \ldots, d_\chi$ ist.

Nun verifizieren wir, daß für unser System von Darstellungen $\{M^*_{l,\chi}(\sigma)\}$ von $G(\bar{k}/k)$ alle Bedingungen außer 2) stets erfüllt sind.

1) Sei $\mathfrak{m}$ das Produkt aller Primideale $\mathfrak{p}$ in k, die unzulässig für J sind. Da es endlich viele Primideale sind, ist $\mathfrak{m}$ ein ganzes Ideal in k. Aus der Reduktionstheorie folgt dann $M^*_{l,\chi}(\sigma_\mathfrak{B}) \sim M^*_{l,\chi}(\pi_\mathfrak{p}) = M_l(\varepsilon_\chi \pi_\mathfrak{p})$ für $\mathfrak{p} \in G(\mathfrak{m}l)$, so daß die Matrix $M^*_{l,\chi}(\sigma_\mathfrak{B})$ von $\sigma_\mathfrak{B}$ unabhängig ist.

3) Das charakteristische Polynom von $M^*_{l,\chi}(\sigma_\mathfrak{B})$ für $\mathfrak{B} \in G(\mathfrak{m}l)$ ist dasselbe wie dasjenige von $M^*_{l,\chi}(\pi_\mathfrak{p}) = M_l(\tilde{\varepsilon}_\chi \pi_\mathfrak{p})$, welches andererseits gleich $L(s, \chi, \tilde{K}/\tilde{K}_0)^{r_\chi}$ ist (Satz 9, Teil II), dessen Koeffizienten nach Annahme (da $\varepsilon_\chi \in k_1$ ist) in k_1 liegen.

4) Es gilt $|\tilde{\omega}_i(\mathfrak{p})| = N\mathfrak{p}^{\frac{1}{2}}$ für alle $\mathfrak{p} \in G(\mathfrak{m})$, da $\omega_i(\mathfrak{p})$ auch die Wurzeln des charakteristischen Polynoms von $M_l(\pi_\mathfrak{p})$ sind (Satz 10, Teil II); dies ist eine Folgerung aus der Riemannschen Vermutung.

5) Entweder ist $n_0 = 0$ oder $\tilde{\omega}_i(\mathfrak{p})$ sind ganze algebraische Zahlen, da, wie in 4) $\tilde{\omega}_i(\mathfrak{p})$ Wurzeln des charakteristischen Polynoms von $M_l(\pi_\mathfrak{p})$ sind und dieses Polynom ganzzahlige Koeffizienten mit höchstem Koeffizienten 1 hat.

Um die Bedingung 2) zu erfüllen, setzen wir jetzt folgendes über die Jacobische Mannigfaltigkeit J voraus:

1) $\mathfrak{A}_0(J) \otimes k_1$ enthält eine kommutative halbeinfache Algebra $\mathfrak{C}_\chi$ vom Grad $d_\chi = c_\chi r_\chi \left(= \sigma(\varepsilon_\chi)\right)$ über k_1, die ε_χ als Einheitselement besitzt.

2) Jedes Element von $\mathfrak{C}_\chi \cap \mathfrak{A}(J)$ sei über k definiert.

Wir zeigen jetzt, daß aus diesen Voraussetzungen die Bedingung 2) folgt:

Sei $\mathfrak{C}_\chi = \sum_i L_i \cdot \varepsilon_i$, wo die L_i endliche Erweiterungen von k_1 und ε_i Idempotente in L_i sind. Da ε_χ Einheitselement in $\mathfrak{C}_\chi$ ist, folgt $\varepsilon_\chi = \sum_i \varepsilon_i$ und $\xi = \varepsilon_\chi \xi = \sum_i \xi_i \varepsilon_i$ für

jedes $\xi \in \mathfrak{C}_\chi$. Die Darstellung $\xi = \varepsilon_\chi \xi \to M_l(\varepsilon_\chi \xi)$ von $\mathfrak{C}_\chi$ ist eine treue Darstellung, und die Spur ist folgendermaßen erklärt:

$$\sigma(\xi) = \sigma(\varepsilon_\chi \xi) = \sum_i \nu_i Sp(\xi_i), \quad \text{wo } \sigma(\varepsilon_i) = \nu_i (L_i : k_1)$$

ist. Dabei bedeutet Sp die Spur in der regulären Darstellung von L_i/k_1. Nun gilt

$$\sigma(\varepsilon_\chi) = \sigma\left(\sum_i \varepsilon_i\right) = \sum_i \nu_i (L_i : k_1) = d_\chi.$$

Ferner gilt

$$(\mathfrak{C}_\chi : k_1) = \sum (L_i : k_1) = d_\chi.$$

Durch Vergleich dieser Gleichungen erhalten wir $\nu_i = 1$ für alle i, denn es ist $\nu_i \geqq 0$.

Mit anderen Worten: In der Darstellung $M_l(\xi)$ von $\mathfrak{C}_\chi$ können sämtliche Elemente gleichzeitig auf Diagonalformen gebracht werden.

$\mathfrak{C}_\chi$ geht durch Reduktion modulo $\mathfrak{p}$ mit einem Primideal $\mathfrak{p}$ von k, für welches J keinen Defekt hat, in eine kommutative halbeinfache Algebra $\tilde{\mathfrak{C}}_\chi$ über. $\mathfrak{C}_\chi \to \tilde{\mathfrak{C}}_\chi$ ist ein Isomorphismus, und $\tilde{\mathfrak{C}}_\chi$ ist daher vom Rang d_χ. Die Matrizen $\{M_l(\tilde{\alpha})\}$ mit $\tilde{\alpha} \in \tilde{\mathfrak{C}}_\chi$ können wieder auf Diagonalform gebracht werden, wobei alle von Null verschiedenen Elemente voneinander verschieden sind. Da die Endomorphismen in $\tilde{\mathfrak{C}}_\chi$ wegen (2) über $\tilde{k}_\mathfrak{p}$ definiert sind, ist $\tilde{\varepsilon}_\chi \pi_\mathfrak{p}$ mit allen Elementen $\tilde{\alpha} \in \tilde{\mathfrak{C}}_\chi$ vertauschbar. Infolgedessen kann $M_l(\tilde{\varepsilon}_\chi \pi_\mathfrak{p})$ auf Diagonalform gebracht werden. Die Algebra $\{\tilde{\mathfrak{C}}_\chi, \tilde{\varepsilon}_\chi \pi_\mathfrak{p}\}$ ist wieder kommutativ und halbeinfach, und die Darstellung $\tilde{\alpha} \to M_l(\tilde{\alpha})$ enthält die irreduziblen Darstellungen mit Vielfachheit 1, d. h. sie ist auch vom Rang d_χ, oder, was dasselbe ist, es gilt $\tilde{\varepsilon}_\chi \pi_\mathfrak{p} \in \tilde{\mathfrak{C}}_\chi$. Wegen des Isomorphismus zwischen $\mathfrak{C}_\chi$ und $\tilde{\mathfrak{C}}_\chi$ gibt es ein Element $\pi \in \mathfrak{C}_\chi$ mit dem Bild $\tilde{\varepsilon}_\chi \pi_\mathfrak{p} \in \tilde{\mathfrak{C}}_\chi$.

Für einen Primteiler $\mathfrak{B}$ von $\mathfrak{p}$ in $\bar{k}$ gilt

$$M_l(\varepsilon_\chi \sigma_\mathfrak{B}) = M_{l,\mathfrak{B}}^{-1} \cdot M_l(\tilde{\varepsilon}_\chi \pi_\mathfrak{p}) \cdot M_{l,\mathfrak{B}}.$$

Es ist klar, daß

$$M_l(\pi) = M_{l,\mathfrak{B}}^{-1} \cdot M_l(\tilde{\varepsilon}_\chi \pi_\mathfrak{p}) \cdot M_{l,\mathfrak{B}}$$

ist, und aus beiden folgt $M_l(\varepsilon_\chi \sigma_\mathfrak{B}) = M_l(\pi)$.

Da M_l eine treue Darstellung von $\mathfrak{C}_\chi$ ist, erzeugt $\{M_l(\varepsilon_\chi \sigma_\mathfrak{B})\}$ über k_1' für alle $\mathfrak{B} \in \bar{G}(\mathfrak{m}l)$ eine Algebra $\mathfrak{A}_{l,\chi}$, die isomorph mit einer über k_1 durch alle π (für alle $\mathfrak{p} \in G(\mathfrak{m}l)$) erzeugten Unteralgebra von $\mathfrak{C}_\chi$ ist. Damit haben wir die Bedingung 2) erhalten.

Nach Definition ist die globale Artinsche L-Reihe, die einem Charakter χ zugeordnet ist, durch

$$L(s, \chi, K/K_0)^{r_\chi} = \prod_\mathfrak{p}{}' L(s, \chi, \tilde{K}/\tilde{K}_0)^{r_\chi}$$

gegeben, wo das Produkt auf der rechten Seite über alle zulässigen Primideale $\mathfrak{p}$ von k läuft. Mit anderen Worten: Aus Bedingung 1) folgt wegen der besonderen Wahl von $\mathfrak{m}$

$$\begin{aligned} (51) \qquad L(s, \chi, K/K_0)^{r_\chi} &= \prod_{\mathfrak{p} \in G(\mathfrak{m})} L(s, \chi, \tilde{K}/\tilde{K}_0)^{r_\chi} \\ &= \prod_{\mathfrak{p} \in G(\mathfrak{m})} \left| E - M_l(\tilde{\varepsilon}_\chi \pi_\mathfrak{p}) \cdot N\mathfrak{p}^{-s} \right| \text{ aus (39)} \\ &= \prod_{\mathfrak{p} \in G(\mathfrak{m})} \prod_{i=1}^{d_\chi} (1 - \tilde{\omega}_i(\mathfrak{p}) \cdot N\mathfrak{p}^{-s}). \end{aligned}$$

Bezeichnen ϱ_i die Charaktere von C_k vom Typ (A_0) (als definierender Modul wird $\mathfrak{m}$ genommen), die $(\tilde{\omega}_i(\mathfrak{p}))$ zugeordnet sind, d. h. mit der Eigenschaft $\tilde{\omega}_i(\mathfrak{p}) = \tilde{\varrho}_i(\mathfrak{p})$, dann gilt nach Hecke die Produktentwicklung

$$(52)\qquad \mathfrak{L}(s, \varrho_i, k) = \prod_{\mathfrak{p} \in G(\mathfrak{m})} (1 - \tilde{\varrho}_i(\mathfrak{p}) \cdot N\mathfrak{p}^{-s})^{-1}$$
$$= \prod_{\mathfrak{p} \in G(\mathfrak{m})} (1 - \tilde{\omega}_i(\mathfrak{p}) \cdot N\mathfrak{p}^{-s})^{-1} \qquad (i = 1, \ldots, d_\chi)$$

($\mathfrak{L}(s, \varrho_i, k)$ bezeichnet die L-Reihe mit *Größencharakter* ϱ_i in k).

Aus (51) und (52) haben wir endlich

$$(53)\qquad L(s, \chi, K/K_0)^{r_\chi} = \prod_{i=1}^{d_\chi} \mathfrak{L}(s, \varrho_i, k)^{-1}.$$

Bemerkungen: 1) Die Bedingungen von Taniyama lassen sich als Spezialfall der obigen folgern, wenn wir $K = K_0$ und $\chi = 1$ nehmen. Dann ist $\varepsilon_\chi = 1$ und die Algebra $\mathfrak{C}_\chi$ ist von der Dimension $\sigma(1) = 2g$.

2) Wenn für das System $\{M_l^*(\sigma_{\mathfrak{P}})\}$ die Bedingung ($\mathrm{CA}'_{\mathrm{II}}$) von Taniyama [11] erfüllt ist, dann ist unsere Bedingung 2) für alle χ erfüllt, wenn wir als Algebra das Bild dieser Algebra nehmen, das durch Multiplikation mit ε_χ entsteht, und umgekehrt, wenn unsere Bedingung für alle χ erfüllt ist und wenn wir die direkte Summe nehmen, erhalten wir die Bedingung ($\mathrm{CA}'_{\mathrm{II}}$) von Taniyama. Das bedeutet nur, daß $\zeta(s, K)$ dann und nur dann ein Produkt von L-Reihen mit Größencharakteren in k ist, wenn das gleiche für $L(s, \chi, K/K_0)^{r_\chi}$ mit jedem χ gilt. Mit anderen Worten, sie ist nur eine Neuformulierung des Satzes 10 von Teil III, der besagt, daß $\zeta(s, K) = \prod_\chi L(s, \chi, K/K_0)^{r_\chi}$ ist.

Teil V.

§ 8. Einige Beispiele.

Wir kehren jetzt zu dem Fall in Teil III zurück und beschränken uns auf spezielle Primzahlstufen q und spezielle Charaktere χ. Wir beweisen, daß die entsprechende globale Artinsche L-Reihe sich als ein Produkt von L-Reihen mit Größencharakteren in $k = Q(\zeta_q)$ darstellen läßt. (Aus der Bemerkung am Ende wird folgen, wie dieser Satz mit dem Resultat von Teil IV zusammenhängt.)

Wir nehmen von jetzt ab $q \equiv 3 \pmod 4$ an. Die einzigen irreduziblen Darstellungen vom zweiten Typus sind dann die zwei konjugierten Darstellungen D_1, D_2 der Dimension $\frac{q-1}{2}$. Wenn $\varkappa_1$, $\varkappa_2$ ihre Vielfachheiten in der Darstellung M^d sind, gilt nach Hecke immer $\varkappa_1 - \varkappa_2 = h$ (Klassenzahl von $Q(\sqrt{-q})$). Aber für manche Werte von q, z. B. $q = 7, 11, 19, 23, 31, 47, 71$ gilt auch $\varkappa_1 + \varkappa_2 = h$, d. h. für diese Primzahlen ist $\varkappa_1 = h$, $\varkappa_2 = 0$, [6]. Wir werden uns nur mit diesen Primzahlen beschäftigen.

Aus Teil III erhalten wir folgendes: Für die dem Charakter $\chi_0 = \chi_1 + \chi_2$ zugeordnete globale Artinsche L-Reihe gilt:

$$L(s, \chi_0, K_q/R_q)^2 = \prod_p{}' \prod_{\varrho=1}^{f_p}{}' \big[\,|\, E - \gamma(p)\, p^{-s} \varepsilon^\varrho + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho} \,|$$
$$\cdot \,|\, E - \overline{\gamma(p)}\, p^{-s} \varepsilon^\varrho + \overline{\varepsilon(p)}\, E p^{1-2s} \varepsilon^{2\varrho} \,| \big].$$

Wenn $\Phi_i(s) = \Phi_i(s, \eta_i)$ $\left(i = 1, \ldots, \frac{q-1}{2}\right)$ die (h, h)-Matrix von Dirichletreihen bezeichnet, die dem Formenraum zugeordnet ist, der zu $D_1 + D_2$ und dem Charakter $\eta_i(n) = \varepsilon_i(n^2) \cdot \varepsilon(n)$ gehört, dann gilt:

$$(54)\qquad |\, \Phi_i(s) \,| = \prod_{\substack{p \\ (p \neq q)}} |\, E - \gamma(p)\, p^{-s} \varepsilon_i(p) + \varepsilon(p)\, \varepsilon_i(p^2)\, E p^{1-2s} \,|^{-1},$$

wobei man alle $|\, \Phi_i(s) \,|$ erhält, wenn man alle Charaktere η_i der Gruppe nimmt.

Für $\Phi(s) = \prod_{i=1}^{\frac{q-1}{2}} \Phi_i(s)$ erhalten wir aus (54)

$$(55) \qquad |\Phi(s)|^{-1} = \prod_{\substack{p \\ (p \neq q)}} \prod_{\varrho=1}^{f'_p} |E - \gamma(p)\, p^{-s} \cdot \eta^{\varrho} + \varepsilon(p)\, \eta^{2\varrho} E p^{1-2s}|^{g'_p},$$

wo η eine primitive f'_p-te Einheitswurzel ist und f'_p, g'_p folgendermaßen definiert sind:

$$U = G(Q(\zeta_q)/Q(\sqrt{-q})); \; \mathfrak{p} = \mathfrak{p}_1 \cdots \mathfrak{p}_{g'_p}; \; N\mathfrak{p}_i = \mathfrak{p}^{f'_p}.$$

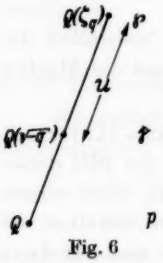


Fig. 6

Wir teilen die Primzahlen p in zwei Arten. Wegen $q \equiv 3 \pmod 4$ können wir folgendermaßen schreiben:

1) $f_p = f'_p$; $g_p = 2g'_p$ oder $p = \mathfrak{p}\mathfrak{p}'$; $\left(\frac{-q}{p}\right) = 1$ oder $\left(\frac{p}{q}\right) = 1$.

2) $f_p = 2f'_p$; $g_p = g'_p$ oder $p = \mathfrak{p}$; $\left(\frac{-q}{p}\right) = -1$ oder $\left(\frac{p}{q}\right) = -1$.

Fall 1. Für Primzahlen dieser Klasse gilt:

$$\prod_{\varrho=1}^{f_p} |E - \gamma(p)\, p^{-s} \varepsilon^{\varrho} + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}|^{g_p} = \prod_{\varrho=1}^{f'_p} |E - \gamma(p)\, p^{-s} \varepsilon^{\varrho} + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}|^{2g'_p}$$
$$= \prod_{\varrho=1}^{f'_p} |E - \gamma(p)\, p^{-s} \eta^{\varrho} + \varepsilon(p)\, E p^{1-2s} \eta^{2\varrho}|^{2g'_p}$$

(wenn man $\eta = \varepsilon$ nimmt).

Fall 2. Wenn die Basisformen F_i als Eigenfunktionen aller Operatoren T_n gewählt sind, folgt nach dem Satz 59 ([5], II) von Hecke, daß $F_i \mid T_p = 0$ für Primzahlen p mit $\left(\frac{p}{q}\right) = -1$ gilt; d. h. für Primzahlen dieser Klasse ist $\gamma(p) = 0$. Also erhalten wir dann

$$\prod_{\varrho=1}^{f_p} |E + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}| = \prod_{\varrho=1}^{2f'_p} |E + \varepsilon(p)\, E p^{1-2s} \eta^{\varrho}| \qquad \text{(wenn man } \varepsilon^2 = \eta \text{ setzt)}$$
$$= \prod_{\varrho=1}^{f'_p} |E + \varepsilon(p)\, E p^{1-2s} \cdot \eta^{\varrho}|^2$$
$$= \prod_{\varrho=1}^{f'_p} |E + \varepsilon(p)\, E p^{1-2s} \eta^{2\varrho}|^2.$$

Da η eine primitive f'_p-te Einheitswurzel ist, ist η^2 wieder eine solche (f'_p ungerade). Also folgt

$$\prod_{\varrho=1}^{f_p} |E + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}|^{g_p} = \prod_{\varrho=1}^{f'_p} |E + \varepsilon(p)\, E p^{1-2s} \eta^{2\varrho}|^{2g'_p}.$$

Aus Fall 1 und Fall 2 schließen wir, daß

$$L(s, \chi_0, K_q/R_q)^2 = \prod_p{}' \prod_{\varrho=1}^{f_p} [\, |E - \gamma(p)\, p^{-s} \cdot \varepsilon^{\varrho} + \varepsilon(p)\, E p^{1-2s} \varepsilon^{2\varrho}|$$
$$\cdot\, |E - \overline{\gamma(p)}\, p^{-s} \cdot \varepsilon^{\varrho} + \overline{\varepsilon(p)}\, E p^{1-2s} \varepsilon^{2\varrho}|]^{g_p}$$
$$= f_1(s) \cdot (\, |\Phi(s)| \cdot |\tilde{\Phi}(s)|\,)^{-2}$$

gilt, wo $\tilde{\Phi}(s)$ aus $\Phi(s)$ nach dem Ersetzen von $\gamma(p)$ und $\varepsilon(p)$ durch $\overline{\gamma(p)}$ bzw. $\overline{\varepsilon(p)}$ entsteht und $f_1(s)$ eine rationale Funktion von p^{-s} ist. Damit bekommen wir endlich

$$(56) \qquad L(s, \chi_0, K_q/R_q) = (\, |\Phi(s)| \cdot |\tilde{\Phi}(s)|\,)^{-1} \cdot f(s),$$

und daraus folgt, daß $L(s, \chi_0, K_q/R_q)$ eine meromorphe Funktion von s ist.

Nun zeigen wir, daß $|\Phi(s)|$ und $|\tilde{\Phi}(s)|$ sich als Produkte von L-Reihen mit Größencharakteren in $Q(\zeta_q)$ darstellen lassen. Nach Hecke haben wir $h \cdot \frac{q-1}{2}$ kanonische Eulerprodukte $f_i(s)$ der Matrix $\Phi(s)$, und zwar gilt ([5], II):

$$(57) \qquad |\Phi(s)| = \prod_{i=1}^{h \cdot \frac{q-1}{2}} f_i(s) = \prod_{\psi} \prod_{\mathfrak{p}}{}' \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\mathfrak{p})}{(N\mathfrak{p})^{s-\frac{1}{2}}}\right)^{-1},$$

wo in den Produkten ψ über alle Charaktere der Idealklassengruppe mod $\sqrt{-q}$ und $\mathfrak{p}$ über alle Primideale $(\neq \sqrt{-q})$ von $Q(\sqrt{-q})$ läuft. Dabei ist $\lambda(\mathfrak{p})$ der Charakter der Gruppe $G(\sqrt{-q})$, der durch den Größencharakter λ von $Q(\sqrt{-q})$ induziert wird. Der Größencharakter λ ist durch die Forderung $\lambda(\alpha) = \frac{\alpha}{|\alpha|}$ für Elemente $\alpha \in Q(\sqrt{-q})$ eindeutig bestimmt. Nach der Definition der L-Reihen mit Größencharakteren folgt aus (57), daß dann

$$(58) \qquad |\Phi(s)| = \prod_{\psi'} \mathfrak{L}(s - \tfrac{1}{2}, \psi', Q(\sqrt{-q}))$$

gilt, wo ψ' die Größencharaktere $\lambda \cdot \psi$ von $Q(\sqrt{-q})$ bedeuten.

Wir werden jetzt zwei Sätze beweisen, aus welchen das gesuchte Resultat folgt:

Satz 14. *Es gilt:*

$$1) \qquad \prod_{\psi'} \mathfrak{L}(s - \tfrac{1}{2}, \psi', Q(\sqrt{-q})) = \mathfrak{L}(s - \tfrac{1}{2}, \hat{\lambda}, H_q),$$

wo H_q den Strahlklassenkörper modulo $\sqrt{-q}$ bedeutet, der Größencharakter $\hat{\lambda}$ des Körpers H_q durch

$$\hat{\lambda}(\mathfrak{P}) = \lambda(N_{H_q/Q(\sqrt{-q})}\mathfrak{P})$$

erklärt und der definierende Modul $\sqrt{-q}$ ist.

$$2) \qquad \mathfrak{L}(s - \tfrac{1}{2}, \hat{\lambda}, H_q) = \prod_{i=1}^{h} \mathfrak{L}(s - \tfrac{1}{2}, \mu_i, Q(\zeta_q)),$$

wo μ_i gewisse Größencharaktere des Körpers $Q(\zeta_q)$ sind, die durch $\hat{\lambda}$ definiert werden.

Beweis. 1) Sei $\mathfrak{p}$ ein beliebiges Primideal $(\neq \sqrt{-q})$ in $Q(\sqrt{-q})$. Dann gilt

$$\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_{g_\mathfrak{p}} \text{ und } N\mathfrak{P}_i = \mathfrak{p}^{f_\mathfrak{p}};\ h \cdot \frac{q-1}{2} = f_\mathfrak{p} \cdot g_\mathfrak{p}.$$

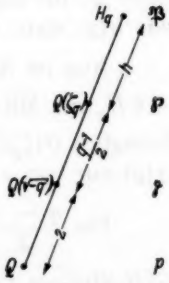


Fig. 7

Wir betrachten jetzt das Produkt

$$\prod_{\psi} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\mathfrak{p})}{(N\mathfrak{p})^{s-\frac{1}{2}}}\right)^{-1}.$$

Nun gilt $\psi(\mathfrak{p}) \neq 0$ nur für diejenigen $\mathfrak{p}$, für die $\mathfrak{p} \nmid \mathfrak{f}(\psi)$ ist ($\mathfrak{f}$ ist der Führer von ψ). Bezeichnet man diese Charaktergruppe mit $\mathfrak{R}_\mathfrak{p}$, so hat $\mathfrak{R}_\mathfrak{p}$ die Ordnung $f_\mathfrak{p} \cdot g_\mathfrak{p}$, und die Untergruppe $U_\mathfrak{p}$ der Charaktere $\psi \in \mathfrak{R}_\mathfrak{p}$ mit $\psi(\mathfrak{p}) = 1$ hat die Ordnung $g_\mathfrak{p}$. Die Faktorgruppe $\mathfrak{R}_\mathfrak{p}/U_\mathfrak{p}$ ist dann eine zyklische Gruppe der Ordnung $f_\mathfrak{p}$.

Jetzt schreiben wir das Produkt folgendermaßen um:

$$\prod_{\mathfrak{p}} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\mathfrak{p})}{(N\mathfrak{p})^{s-\frac{1}{2}}}\right) = \prod_{\substack{\zeta \\ \zeta^{f_\mathfrak{p}} = 1}} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \zeta}{(N\mathfrak{p})^{s-\frac{1}{2}}}\right)^{g_\mathfrak{p}}$$

$$= \left(1 - \frac{(\lambda(\mathfrak{p}))^{f_\mathfrak{p}}}{(N\mathfrak{p}^{f_\mathfrak{p}})^{s-\frac{1}{2}}}\right)^{g_\mathfrak{p}}$$

$$= \prod_{\mathfrak{P} \mid \mathfrak{p}} \left(1 - \frac{\lambda(N_{H_q/Q(\sqrt{-q})}\, \mathfrak{P})}{(N_{H_q/Q}\, \mathfrak{P})^{s-\frac{1}{2}}}\right)$$

Das Produkt auf beiden Seiten über $\mathfrak{p}$ liefert dann den Teil 1).

2) Wegen der Struktur des Strahlklassenkörpers H_q modulo $\sqrt{-q}$ ist die Galoisgruppe $G(H_q/Q(\sqrt{-q}))$ das direkte Produkt von $G(H_q/Q(\zeta_q))$ und $G(Q(\zeta_q)/Q(\sqrt{-q}))$. Jeder Charakter χ der Gruppe $G(H_q/Q(\zeta_q))$ läßt sich zu einer Darstellung der Gruppe $G(H_q/Q(\sqrt{-q}))$, sogar zu einer $\frac{q-1}{2}$-dimensionalen Darstellung, erweitern. Diese Darstellung ist offenbar irreduzibel, und wir bezeichnen die Spur dieser Darstellung mit ψ_χ. ψ_χ zerlegt sich in eine Summe von $\frac{q-1}{2}$ einfacheren Charakteren der Gruppe $G(H_q/Q(\sqrt{-q}))$.

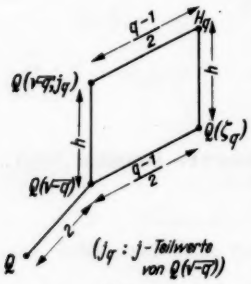


Fig. 8

Wir behaupten dann

$$(59) \quad \prod_{\wp \mid \mathfrak{p}} \left(1 - \frac{\mu_i(\wp)}{(N\wp)^s}\right) = \prod_{\psi \in \psi_\chi} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\mathfrak{p})}{(N\mathfrak{p})^s}\right).$$

Auf der linken Seite läuft das Produkt über alle Primideale von $Q(\zeta_q)$, die in $\mathfrak{p}$ aufgehen, und die μ_i sind Größencharaktere des Körpers $Q(\zeta_q)$, für die $\mu_i(\wp) = \hat{\lambda}(\wp) \cdot \chi(\wp)$ mit

$$\hat{\lambda}(\wp) = \lambda(N_{Q(\zeta_q)/Q(\sqrt{-q})}\wp) \text{ und } \chi(\wp) = \chi(\sigma_\wp)$$

gilt, wo $\sigma_\wp$ die Frobeniussche Substitution von $\wp$ ist. Wenn χ über alle h Charaktere der Gruppe $G(H_q/Q(\zeta_q))$ läuft, dann läuft i von 1 bis h.

Bedeutet $\sigma_\mathfrak{P}$ die Frobeniussche Substitution in $G(H_q/Q(\sqrt{-q}))$, dann gilt $\sigma A \equiv A^{N\mathfrak{p}}$ (mod $\mathfrak{P}$) für alle $A \in H_q$. Da $H_q/Q(\sqrt{-q})$ abelsch ist, hängt $\psi(\sigma_\mathfrak{P})$ nur von $\mathfrak{p}$ ab, so daß wir $\psi(\mathfrak{p})$ statt $\psi(\sigma_\mathfrak{P})$ schreiben können.

Nun ist $N\wp = N\mathfrak{p}^{f_\mathfrak{p}}$ für alle $\wp \mid \mathfrak{p}$ in $Q(\zeta_q)$, so daß $\sigma_\mathfrak{P}^{f_\mathfrak{p}} \cdot A \equiv A^{N\wp}$(mod $\mathfrak{P}$) für alle $A \in H_q$ gilt. Mit anderen Worten, $\sigma_\mathfrak{P}^{f_\mathfrak{p}}$ ist die Frobeniussche Substitution des Primideals $\mathfrak{P}$ bezüglich $Q(\zeta_q)$. $\sigma_\mathfrak{P}^{f_\mathfrak{p}}$ gehört dann zu $G(H_q/Q(\zeta_q))$. Wir setzen $\chi(\wp) = \chi(\sigma_\mathfrak{P}^{f_\mathfrak{p}})$. Dann ist $\chi(\wp)$ nur von $\wp$ und nicht von $\mathfrak{P}$ abhängig.

Die $\frac{q-1}{2}$ Charaktere ψ, die in ψ_χ enthalten sind, sind, wenn man sie auf $G(H_q/Q(\sqrt{-q}, j_q))$ einschränkt, alle $\frac{q-1}{2}$ Charaktere dieser Gruppe und können als Charaktere der Gruppe $G(Q(\zeta_q)/Q(\sqrt{-q}))$ betrachtet werden, denn es ist

$$G(H_q/Q(\sqrt{-q}, j_q)) \cong G(Q(\zeta_q)/Q(\sqrt{-q})).$$

Aus dem direkten Produkt

$$G(H_q/Q(\sqrt{-q})) \cong G(H_q/Q(\sqrt{-q}, j_q)) \times G(H_q/Q(\zeta_q))$$

folgt $\sigma_{\mathfrak{P}} = \sigma_{1\mathfrak{P}} \cdot \sigma_{2\mathfrak{P}}$ mit $\sigma_{1\mathfrak{P}} \in G(H_q/Q(\sqrt{-q}, j_q))$ und $\sigma_{2\mathfrak{P}} \in G(H_q/Q(\zeta_q))$, so daß $\psi(\sigma_{\mathfrak{P}}) = \psi(\sigma_{1\mathfrak{P}}) \cdot \psi(\sigma_{2\mathfrak{P}})$ gilt. Da $\sigma_{\mathfrak{P}}^{f'_{\mathfrak{p}}} = \sigma_{1\mathfrak{P}}^{f'_{\mathfrak{p}}} \cdot \sigma_{2\mathfrak{P}}^{f'_{\mathfrak{p}}}$ und $\sigma_{\mathfrak{P}}^{f'_{\mathfrak{p}}} \in G(H_q/Q(\zeta_q))$ ist, gilt $\sigma_{\mathfrak{P}}^{f'_{\mathfrak{p}}} = \sigma_{2\mathfrak{P}}^{f'_{\mathfrak{p}}}$ und $\sigma_{1\mathfrak{P}}^{f'_{\mathfrak{p}}} = 1$. Folglich ist $\psi(\sigma_{1\mathfrak{P}})$ eine $f'_{\mathfrak{p}}$-te Einheitswurzel.

Wir behaupten jetzt, daß $\sigma_{1\mathfrak{P}}$ die Frobeniussche Substitution von $\wp$ in

$$G(Q(\zeta_q)/Q(\sqrt{-q})),$$

d. h. das isomorphe Bild in $G(Q(\zeta_q)/Q(\sqrt{-q})$, ist.

Es ist $\sigma_{\mathfrak{P}} A \equiv A^{N\mathfrak{p}} (\mathrm{mod}\ \mathfrak{P})$ für alle $A \in H_q$. Für $A \in Q(\zeta_q)$ gilt

$$\sigma_{\mathfrak{P}} \cdot A = (\sigma_{1\mathfrak{P}} \cdot \sigma_{2\mathfrak{P}})\, A = \sigma_{1\mathfrak{P}} \cdot A\,,$$

da $\sigma_{2\mathfrak{P}} \in G(H_q/Q(\zeta_q))$ ist, so daß $\sigma_{1\mathfrak{P}} \cdot A \equiv A^{N\mathfrak{p}} (\mathrm{mod}\ \mathfrak{P})$ und daher auch mod $\wp$ gilt (denn es ist $\mathfrak{P} \cap Q(\zeta_q) = \wp$). Also schreiben wir $\Phi(\wp)$ statt $\psi(\sigma_{1\mathfrak{P}})$. Zusammenfassend erhalten wir

$$\begin{aligned}
\prod_{\psi \in \Psi_\chi} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\mathfrak{p})}{(N\mathfrak{p})^s}\right) &= \prod_{\psi \in \Psi_\chi} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\sigma_{1\mathfrak{P}} \cdot \sigma_{2\mathfrak{P}})}{(N\mathfrak{p})^s}\right) \\
&= \prod_{\Phi} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \Phi(\wp) \cdot \psi(\sigma_{2\mathfrak{P}})}{(N\mathfrak{p})^s}\right) \\
&= \prod_{\substack{\zeta \\ \zeta^{f'_{\mathfrak{p}}} = 1}} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \zeta \cdot \psi(\sigma_{2\mathfrak{P}})}{(N\mathfrak{p})^s}\right)^{g'_{\mathfrak{p}}} \\
&= \left(1 - \left(\frac{\lambda(\mathfrak{p}) \cdot \psi(\sigma_{2\mathfrak{P}})}{(N\mathfrak{p})^s}\right)^{f'_{\mathfrak{p}}}\right)^{g'_{\mathfrak{p}}} \\
&= \left(1 - \frac{\lambda(\mathfrak{p})^{f'_{\mathfrak{p}}} \cdot \psi(\sigma_{\mathfrak{P}}^{f'_{\mathfrak{p}}})}{(N\mathfrak{p}^{f'_{\mathfrak{p}}})^s}\right)^{g'_{\mathfrak{p}}} \\
&= \prod_{\wp \mid \mathfrak{p}} \left(1 - \frac{\lambda(N_{Q(\zeta_q)/Q(\sqrt{-q})}\, \wp) \cdot \chi(\wp)}{(N\wp)^s}\right),
\end{aligned}$$

wo $\psi(\sigma_{2\mathfrak{P}}^{f'_{\mathfrak{p}}}) = \psi(\sigma_{\mathfrak{P}}^{f'_{\mathfrak{p}}}) = \chi(\wp)$ und $\mathfrak{p} = \wp_1 \cdots \wp_{g'_{\mathfrak{p}}}$ gilt. Das beweist dann (59).

Das Produkt von (59) über alle Primideale $\mathfrak{p}(\neq \sqrt{-q})$ liefert

$$\prod_{\mathfrak{p}}{}' \prod_{\psi \in \Psi_\chi} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\mathfrak{p})}{(N\mathfrak{p})^{s-\frac{1}{2}}}\right)^{-1} = \prod_{\mathfrak{p}}{}' \prod_{\wp \mid \mathfrak{p}} \left(1 - \frac{\lambda(N\wp) \cdot \chi(\wp)}{(N\wp)^{s-\frac{1}{2}}}\right)^{-1}.$$

Das Produkt über alle Charaktere χ von $G(H_q/Q(\zeta_q))$ ergibt daraus

$$\begin{aligned}
\prod_{\chi} \prod_{\mathfrak{p}}{}' \prod_{\psi \in \Psi_\chi} \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\mathfrak{p})}{N(\mathfrak{p})^{s-\frac{1}{2}}}\right)^{-1} &= \prod_{\psi} \prod_{\mathfrak{p}}{}' \left(1 - \frac{\lambda(\mathfrak{p}) \cdot \psi(\mathfrak{p})}{N(\mathfrak{p})^{s-\frac{1}{2}}}\right)^{-1} \\
&= \prod_{\psi'} \mathfrak{L}\left(s - \tfrac{1}{2},\ \psi',\ Q(\sqrt{-q})\right)
\end{aligned}$$

und

$$\prod_{\chi} \prod_{\wp}{}' \left(1 - \frac{\mu_i(\wp)}{(N\wp)^{s-\frac{1}{2}}}\right)^{-1} = \prod_{i=1}^{h} \mathfrak{L}\left(s - \tfrac{1}{2},\ \mu_i,\ Q(\zeta_q)\right).$$

Die beiden obigen Gleichungen zusammen implizieren unsere Behauptung 2).

Aus (58) erhalten wir

$$|\Phi(s)| = \prod_{\psi'} \mathfrak{L}\left(s - \tfrac{1}{2},\ \psi',\ Q(\sqrt{-q})\right) = \prod_{i=1}^{h} \mathfrak{L}\left(s - \tfrac{1}{2},\ \mu_i,\ Q(\zeta_q)\right).$$

Aus der Struktur von $\widetilde{\Phi}(s)$ folgt sofort, daß

$$|\widetilde{\Phi}(s)| = \prod_{i=1}^{h} \mathfrak{L}(s - \tfrac{1}{2}, \bar{\mu}_i, Q(\zeta_q))$$

gilt, so daß wir endlich für die globale Artinsche L-Reihe

$$(60) \qquad L(s, \chi_0, K_q/R_q) = f(s) \prod_{i=1}^{h} \mathfrak{L}(s - \tfrac{1}{2}, \mu_i, Q(\zeta_q))^{-1} \mathfrak{L}(s - \tfrac{1}{2}, \bar{\mu}_i, Q(\zeta_q))^{-1}$$

bekommen.

Bemerkungen:

1) Die obige Zerlegung kann auch indirekt aus den Resultaten von Teil IV hergeleitet werden. Die kommutative, halbeinfache Algebra $\mathfrak{C}_{\chi_0}$ besteht aus der Menge aller $\{\varepsilon_{\chi_0} \xi_p\}$. Man sieht leicht, daß die Größencharaktere in (60) sogar vom Typ (A_0) sind.

2) Aus dem Zerlegungsgesetz (Satz 10 von Teil II) folgt für die globale Artinsche L-Reihe auch ein Zerlegungsgesetz, und nach (50) und (60) gilt

$$\zeta(s, K_q) = \prod_{\chi} L(s, \chi, K_q/R_q)^{r_\chi} \qquad (\chi = \chi_0, \text{ wenn } \chi \text{ vom } r\text{-ten Typus ist})$$

$$= \zeta(s, T_q)^q \cdot L(s, \chi_0, K_q/R_q)^{\frac{q-1}{2}} \cdot g(s),$$

indem man die übrigen Faktoren zu $g(s)$ zusammenfaßt.

Für $q = 11, 19$ ist der Körper T_q vom Geschlechte 1 und somit ein elliptischer Funktionenkörper, und außerdem hat dieser Körper keine (nicht-trivialen) komplexen Multiplikationen. Im allgemeinen ist nicht bekannt, ob $\zeta(s, T_q)$ ein Produkt von Heckeschen L-Reihen ist; aber aus (60) folgt, daß die Reihe $L(s, \chi_0, K_q/R_q)$ sich als Produkt von Heckeschen L-Reihen darstellen läßt.

Anhang.

Berechnung der Vielfachheit einer irreduziblen Darstellung.

Es sei $\mathfrak{N}$ eine normale Untergruppe von $\Gamma(1)$ mit endlichem Index μ. Wir nehmen ferner an, daß $\mathfrak{N}$ vom Verzweigungsschema $(2, 3, N)$ ist (*Fricke-Klein*, Automorphe Funktionen, Bd. I, 333—343), wo N die kleinste Zahl ist, für die $U^N \in \mathfrak{N}$ mit $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ist. Dies bedeutet dann, daß $\mathfrak{N}$ keine elliptischen Ecken besitzt und das Geschlecht p von $\mathfrak{N}$ positiv ist. Es gilt sogar $p = 1 + \frac{\mu}{12N}(N - 6)$.

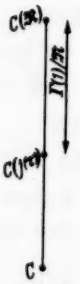


Fig. 9

Bezeichnen wir mit $C(\mathfrak{N})$ den Körper der in der oberen Halbebene meromorphe Funktionen, die unter den Substitutionen von $\mathfrak{N}$ invariant bleiben. $C(\mathfrak{N})$ ist dann ein algebraischer Funktionenkörper einer Variablen über C. Ferner ist $C(\mathfrak{N})$ eine Galoissche Erweiterung von $C(j(\tau))$ mit der zu $\Gamma(1)/\mathfrak{N}$ isomorphen Galoisgruppe.

Es sei D eine absolut irreduzible Darstellung von $\Gamma(1)/\mathfrak{N}$ und $\varkappa(D)$ die Vielfachheit von D in der Darstellung M^d im Raum der Differentiale erster Gattung. Es ist leicht einzusehen, daß $\varkappa(D) + \overline{\varkappa(D)}$ nichts anderes als die Vielfachheit von D in der l-adischen Darstellung von $\Gamma(1)/\mathfrak{N}$, betrachtet als Gruppe von Korrespondenzen bzw. Korrespondenzklassen, ist.

Nach Weil ([13], S. 79) wissen wir dann, daß diese Vielfachheit c_χ ist, die ihrerseits folgendermaßen definiert ist:

$$c_\chi = (2p_0 - 2)r_\chi + \operatorname{grad} \mathfrak{f}_\chi + 2\varrho_\chi,$$

wo χ der Charakter von D, $r_\chi = \chi(1)$, p_0 das Geschlecht des Unterkörpers, $\mathfrak{f}_\chi$ der Artinsche Führer von χ und $\varrho_\chi = 1$ oder 0 ist (je nachdem, ob $\chi = 1$ oder $\chi \neq 1$ ist). In unserem Fall ist $p_0 = 0$, und wenn wir uns auf $\chi \neq 1$ beschränken, ist $\varrho_\chi = 0$. Es folgt dann

$$\varkappa(D) + \overline{\varkappa(D)} = c_\chi = \operatorname{grad} \mathfrak{f}_\chi - 2r_\chi.$$

Die Zahl $\varkappa(D) + \overline{\varkappa(D)}$ wurde von Hecke [6] bestimmt. Wir werden hier einen direkten kurzen Beweis für das Resultat von Hecke geben.

Wir werden den Artinschen Führer $\mathfrak{f}_\chi$ für diesen Fall explizit bestimmen und daraus den Grad ausrechnen.

Bezeichnen wir zuerst mit $S_{\mathfrak{N}}$ die den $C(\mathfrak{N})$ zugeordnete Riemannsche Fläche und mit S die Riemannsche Kugel. $S_{\mathfrak{N}}$ ist dann eine verzweigte Überlagerungsfläche von S und es wird sogar folgendes bewiesen:

1) Die Verzweigungspunkte in $S_{\mathfrak{N}}$ liegen über den drei Punkten $i\,\infty$, $\omega = e^{2\pi i/3}$ und i in S mit den Verzweigungsindizes N, 3 und 2.

2) Die Trägheitsgruppen an diesen Stellen (betrachtet als Primstellen von $C(j(\tau))$ sind die Gruppen $(\overline{U}^n,\ 0 \leqq n < N)$, $(\overline{TU}^n,\ 0 \leqq n < 3)$ und $(\overline{T}^n,\ 0 \leqq n < 2)$ mit den Ordnungen N, 3 und 2. (Hier bedeuten $\overline{U}$, $\overline{TU}$, $\overline{T}$ die Restklassen von U, TU und T modulo $\mathfrak{N}$).

3) Für jede dieser Primstellen sind die Hilbert-Verzweigungsgruppen V_i $(i > 0)$ trivial, d. h. die einzige nicht-triviale Verzweigungsgruppe ist $V_0 = \mathfrak{T}$ (Trägheitsgruppe).

Beweis. 1) Da $\mathfrak{N}$ vom Verzweigungsschema (2, 3, N) ist, folgt sofort, daß die Verzweigungspunkte auf S die Punkte $i\,\infty$, ω und i mit den Verzweigungsindizes N, 3 und 2 sind.

2) Nun, da C algebraisch abgeschlossen ist, gilt $f_P = 1$ für alle Primstellen P von $C(j(\tau))$, so daß die Zerlegungsgruppe von P mit der Trägheitsgruppe von P übereinstimmt. Aber definitionsgemäß besteht die Zerlegungsgruppe aus Automorphismen φ mit $P^\varphi = P$, d. h. den Elementen von $\Gamma(1)/\mathfrak{N}$, die P fixieren. Das impliziert dann unsere Behauptung 2).

3) Es genügt, unsere Behauptung 3) für die Primstelle $i\,\infty$ zu beweisen, da die Trägheitsgruppen an den Stellen ω und i von Primzahlordnung sind. Für die Stelle $i\,\infty$ sei $f(\tau)$ eine lokale Uniformisierende. Da $U^N \in \mathfrak{N}$ ist, gilt $f(\tau + N) = f(\tau)$. $f(\tau)$ besitzt dann eine Fourierentwicklung

$$f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i \frac{n\tau}{N}}.$$

Wegen unserer Voraussetzungen gilt $a_0 = 0$, $a_1 \neq 0$. Für ein λ mit $0 \leqq \lambda < N$ gilt

$$f(\tau + \lambda) - f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i \frac{n\tau}{N}} \left(e^{2\pi i \frac{n\lambda}{N}} - 1\right)$$

$$= \sum_{n=1}^{\infty} a'_n e^{2\pi i \frac{n\tau}{N}},$$

wo $a'_n = a_n\left(e^{2\pi i \frac{n\lambda}{N}} - 1\right)$ ist. Da $a_1 \neq 0$ ist, gilt $a'_1 = 0$ nur dann, wenn $\lambda \equiv 0 \pmod N$ ist, d. h. die erste Verzweigungsgruppe V_1 ist gleich (1). Infolgedessen sind die übrigen auch gleich (1).

Nun gilt nach der Definition des Führers von *Artin* (J. f. reine u. angew. Math. **164** [1931], S. 1) in unserem Fall

$$\operatorname{Grad} \mathfrak{f}_\chi = \sum_P \left(\chi(1) - \frac{1}{e}\,\chi(\mathfrak{T})\right),$$

da Grad $P = 1$ ist und die höheren Verzweigungsgruppen trivial sind. $\mathfrak{T}$ ist die Trägheitsgruppe (der Ordnung e) an der Stelle P und $\chi(\mathfrak{T}) = \sum_{\sigma \in \mathfrak{T}} \chi(\sigma)$.

Aus 2) folgt dann

$$\operatorname{Grad} \mathfrak{f}_\chi = 3r_\chi - \frac{1}{N} \sum_{n \bmod N} \chi(\bar{U}^n) - \frac{1}{2} \sum_{n \bmod 2} \chi(\bar{T}^n) - \frac{1}{3} \sum_{n \bmod 3} \chi(\overline{TU}^n)$$

und daraus für c_χ:

$$\begin{aligned} c_\chi &= \operatorname{Grad} \mathfrak{f}_\chi - 2r_\chi \\ &= \chi(1) - \frac{1}{N} \sum_{n \bmod N} \chi(\bar{U}^n) - \frac{1}{2} \sum_{n \bmod 2} \chi(\bar{T}^n) - \frac{1}{3} \sum_{n \bmod 3} \chi(\overline{TU}^n). \end{aligned}$$

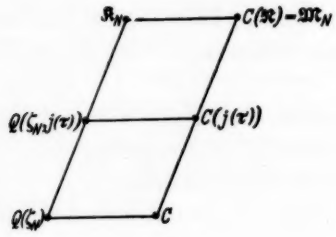


Fig. 10

Bemerkung: Im Fall $\mathfrak{N} = \Gamma_1(N)$ wie in Teil I, haben wir einen Funktionenkörper $\mathfrak{K}_N$, der über C die Körper $C(\mathfrak{N})\,(= \mathfrak{M}_N)$ erzeugt. Die Zahl c_χ bleibt definitionsgemäß für $\mathfrak{K}_N$ sowie für $\mathfrak{M}_N$ dieselbe, so daß der oben bestimmte Ausdruck c_χ auch für das c_χ bezüglich $\mathfrak{K}_N$ gilt.

Literatur.

[1] *M. Deuring*, Reduktion algebraischer Funktionenkörper nach Primdivisoren des Konstantenkörpers, Math. Z. **47** (1942), 643—654.

[2] *M. Deuring*, Die Struktur der elliptischen Funktionenkörper und die Klassenkörper der imaginären quadratischen Zahlkörper, Math. Ann. **124** (1951/52), 393—426.

[3] *M. Deuring*, Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins (Vierte Mitteilung), Nachr. Akad. Wiss. Göttingen 1957, Math.-Phys. Kl. IIa, 55—80.

[4] *M. Eichler*, Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. Arch. der Math. **5** (1954), 355—366.

[5] *E. Hecke*, Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung I, II, Math. Ann. **114** (1937), 1—28, 316—351; Werke, 644—707.

[6] *E. Hecke*, Grundlagen einer Theorie der Integralgruppen und der Integralperioden bei den Normalteilern der Modulgruppe, Math. Ann. **116** (1939), 469—510; Werke, 731—772.

[7] *P. Roquette*, Arithmetische Untersuchung des Abelschen Funktionenkörpers, der einem algebraischen Funktionenkörper höheren Geschlechts zugeordnet ist. Abh. Math. Sem. Univ. Hamburg **18** (1952), 144—178.

[8] *G. Shimura*, Reduction of algebraic varieties with respect to a discrete valuation of the basic field, Amer. J. Math. **77** (1955), 134—176.

[9] *G. Shimura*, La fonction ζ du corps des fonctions modulaires elliptiques, C. R. Acad. Sci. Paris **244**, 2 (1957); 2127—30.

[10] *G. Shimura*, Correspondances modulaires et les fonctions ζ de courbes algébriques, Journ. Math. Soc. of Japan **10** (1958), 1—28.

[11] *Y. Taniyama*, *L*-functions of number fields and zeta functions of abelian varieties, Journ. Math. Soc. of Japan **9** (1957), 330—366.

[12] *A. Weil*, Foundations of Algebraic Geometry, New York 1946.

[13] *A. Weil*, Sur les courbes algébriques et les variétés qui s'en deduisent, Actual. Sci. Industr. 1041, Paris 1948.

[14] *A. Weil*, Variétés abéliennes et courbes algébriques, Actual. Sci. Industr. 1064, Paris 1948.

[15] *A. Weil*, On the theory of complex multiplication, Proc. International Symposium on algebraic number theory, Tokyo-Nikko 1955, 9—22.

Eingegangen 7. Oktober 1959.

Spaces that admit a category measure.

By *John C. Oxtoby* in Bryn Mawr (Pa.), U.S.A.

1. Introduction.

A *category measure* in a topological space is a finite, countably additive measure m defined on the class of sets having the property of Baire and such that $m(E) = 0$ if and only if E is of first category. A space is called *measurable* (more precisely, *category measurable*) if it admits a category measure not identically zero. It is known, for example, that the Boolean space corresponding to any measure algebra is measurable, [4], [8], [9], and that the real line is not measurable [2, p. 186]. In this paper we shall study some properties and examples of category measures and give a construction for all measurable spaces of certain types. At the same time we give a construction for all spaces whose algebra of regular open sets is isomorphic to a specified complete Boolean algebra. We shall also consider an algebraic criterion for a space to have the property that every set of first category is nowhere dense.

The sets having the property of Baire in a space X are those of the form $G + P$, where G is open, P is of first catogory, and "$+$" denotes symmetric difference. These sets constitute a σ-field of subsets of X. The quotient modulo the ideal of sets of first category is called the *category algebra* of X. It is a complete Boolean algebra unless it reduces to a single element.

A Boolean σ-algebra M is called *measurable* if there exists a countably additive, strictly positive measure on M. A measurable algebra is necessarily complete. In any finite measure space the measurable sets modulo the ideal of sets of measure zero constitute a measurable Boolean algebra. Evidently a topological space is measurable if and only if its category algebra is measurable.

In any topological space the open sets and the nowhere dense sets generate a field of subsets of X called the *complete basic ring* of X. It consists of all sets of the form $G + N$, where G is open and N is nowhere dense. If G is required to be *regular open*, that is, such that $G = G^{-\prime -\prime}$, then this representation of any element of the ring is unique. The regular open subsets of X constitute a Boolean algebra $R(X)$ in which the Boolean sum, product, and complement are defined respectively by $(G_1 \cup G_2)^{-\prime -\prime}$, $G_1 \cap G_2$, and $G^{-\prime}$, and the Boolean order relation by set inclusion. We shall call $R(X)$ the *regular algebra* of X. $R(X)$ is isomorphic to the complete basic ring of X reduced modulo the ideal of nowhere dense sets. $R(X)$ is always complete [12, Th. 4. 1].

The mapping that associates to each regular open set G the class of all sets of the form $G + P$, where P is of first category, is a homomorphism of $R(X)$ onto the category algebra of X. This mapping is an isomorphism if and only if X is a *Baire space*, that is, one in which every non-empty open set is of second category. By the Banach Category Theorem [7, p. 49], the union S of all open sets of first category in a topological space X

is itself of first category. Consequently, if $X - S^-$ is non-empty it is an open Baire subspace of X and $R(X - S^-)$ is isomorphic to the category algebra of X. Thus we have the following theorem.

Theorem 1. *Let S be the union of all open sets of first category in a topological space X. X is measurable if and only if $X - S^-$ is non-empty and $R(X - S^-)$ is measurable. In particular, a Baire space is measurable if and only if its regular algebra is measurable.*

In studying measurability we may therefore confine attention to Baire spaces without essential loss of generality.

2. Regularly measurable spaces.

A category measure is defined for all Borel sets, and since every set of first category is contained in an F_σ set of first category it follows that any category measure is the completion of a Borel measure. It is easy to verify that the completion of a finite Borel measure is a category measure if and only if $m(G) = m(G^-)$ for every open set G, and $m(G) > 0$ for every open set of second category. A Borel measure is called *regular* if for each closed set F and positive number ε there exists an open set G such that $F \subset G$ and $m(G) < m(F) + \varepsilon$. A topological space will be called *regularly measurable* if it admits a regular category measure.

We introduce the following definition: a topological space is *quasi-regular* if for each non-empty open set U there exists a non-empty open set V such that $V^- \subset U$. Evidently any regular space is quasi-regular. The converse is not true, nor is there any implication between quasi-regularity and another generalization of regularity, called semi-regularity, introduced by Stone. A space is called *semi-regular* if the regular open sets constitute a base [10, Def. 19]. An example considered by Alexandroff-Hopf [1, p. 31, Beispiel 1°] and by Stone [10, p. 447] shows that a Hausdorff space can be quasi-regular without being semi-regular. (Note, however, that in a quasi-regular space every non-empty open set contains a non-empty regular open set.) A second example considered by Stone [10, p. 453] shows that a Hausdorff space can be quasi-regular and semi-regular without being regular. It is not difficult to modify the latter example so as to obtain a semi-regular Hausdorff space that is not quasi-regular.

Theorem 2. *Let X be a measurable space and let S be the union of all open sets of first category in X. The following assertions concerning X are equivalent:*

1) *some category measure in X is regular;*
2) *every category measure in X is regular;*
3) *$X - S^-$ is a quasi-regular subspace of X.*

In particular, a measurable Baire space is regularly measurable if and only if it is quasi-regular.

Proof. Suppose that m is a regular category measure in X. Let U be any non-empty open set contained in $X - S^-$. Then U is of second category and $m(U) > 0$. Let $F = X - U$. Then $m(F) < m(X)$. Since m is regular there exists an open set W such that $F \subset W$ and $m(W) < m(X)$. Put $V = X - W^-$. Then V is an open set, $V^- \subset X - W \subset U$, and

$$m(V) = m(X) - m(W^-) = m(X) - m(W) > 0.$$

Hence V is a non-empty open subset of U and $V^- \subset U$. Thus 1) implies 3).

Suppose that $Y = X - S^-$ is a quasi-regular subspace of X. Let m be any category measure in X, and let F be any closed subset of X. If F does not contain Y let $\mathcal{F}$ be a

maximal disjoint family of non-empty open sets G such that $G^- \subset Y - F$. The family $\mathcal{F}$ must be countable, say $\mathcal{F} = \{G_i\}$. The maximality of $\{G_i\}$ and the quasi-regularity of Y imply that $\bigcup G_i$ is dense in $Y - F$. Hence $\bigcup G_i$ differs from $Y - F$ by a nowhere dense set, and $m(X - F) = m(Y - F) = \Sigma\, m(G_i)$. For any $\varepsilon > 0$ there is a positive integer n such that $\sum_{i=1}^{n} m(G_i) > m(X - F) - \varepsilon$. Hence $G = \bigcap_{i=1}^{n} (X - G_i^-)$ is an open set containing F, and

$$m(G) = m(X) - m\left(\bigcup_{i=1}^{n} G_i^-\right) \leqq m(F) + m(X - F) - \sum_{i=1}^{n} m(G_i) < m(F) + \varepsilon.$$

On the other hand, if F contains Y then X itself is an open set containing F, and $m(X) = m(F)$. Thus 3) implies 2). Obviously 2) implies 1).

Theorem 3. *If X is a quasi-regular measurable Baire space then every set of first category in X is nowhere dense.*

Proof. By Theorem 2 there exists a regular category measure m in X. Let $\{N_i\}$ be any sequence of nowhere dense sets, with $P = \bigcup N_i$. Then $m(N_i^-) = 0$, and for any $\varepsilon > 0$ there exists a sequence $\{G_i\}$ of open sets such that $N_i^- \subset G_i$ and $m(G_i) \leqq \frac{\varepsilon}{2^i}$ for each i. Let $G = \bigcup G_i$. Then G is open and $m(G^-) = m(G) \leqq \varepsilon$. Since $P^- \subset G^-$ it follows that $m(P^-) \leqq \varepsilon$ for every $\varepsilon > 0$. Hence $m(P^-) = 0$, $m(P^{-\prime-\prime}) = 0$, and therefore $P^{-\prime-\prime}$ is an open set of first category. Because X is a Baire space it follows that $P^{-\prime-\prime}$ is empty, that is, P is nowhere dense.

Theorem 4. *The following assertions concerning a measurable Baire space X are equivalent:*

1) *every set of first category in X is nowhere dense;*

2) *$m(E) = m(E^-) = m(E^{\prime-\prime})$ for every category measure m and every set E having the property of Baire;*

3) *$m(E) = m(E^-)$ (or $m(E) = m(E^{\prime-\prime})$) for some category measure m and for every set E having the property of Baire.*

Proof. Assume 1). Then any set E having the property of Baire is of the form $G + N$, where G is open and N is nowhere dense. Hence

$$G - N^- \subset E^{\prime-\prime} \subset E \subset E^- \subset G^- \cup N^-.$$

Since $m(G - N^-) = m(G^- \cup N^-)$ for any category measure m it follows that 1) implies 2). Obviously 2) implies 3).

Assume 3). Since $m(E) = m(E^-)$ if and only if $m(E') = m(E^{-\prime})$, either version of 3) implies that $m(E) = m(E^-) = m(E^{\prime-\prime})$ for every set E having the property of Baire. In particular, if P is any set of first category then

$$m(P) = m(P^-) = m(P^{-\prime-\prime}) = 0.$$

Hence $P^{-\prime-\prime}$ is an open set of first category, therefore empty, and P is nowhere dense. Thus 3) implies 1).

Two simple examples suffice to show that in a measurable Baire space that is not quasi-regular it may or may not be true that every set of first category is nowhere dense. Let X be an uncountable set. In the first example let the class of closed sets consist of X and its finite subsets. In the second example let the class of closed sets consist of X and its countable subsets. In either case X is a T_1-space, the sets of first category are the countable sets, the sets having the property of Baire are the countable sets and their

complements, and every non-empty open set is of second category. If we define $m(E) = 0$ or 1 according as E or $X - E$ is countable then m is a category measure in either space, but not regular. In the first example the nowhere dense sets constitute a proper subclass of the class of sets of first category. In the second example every set of first category is nowhere dense.

3. Weakly distributive Boolean algebras.

A non-empty subset D of a Boolean algebra A is called a *dual ideal* if $a \in A$, $b \in D$, $c \in D$ imply $a \vee b \in D$ and $b \wedge c \in D$. The intersection of any family of dual ideals is a dual ideal. If a subset E of A has a greatest lower bound in A this will be denoted by $\wedge E$. A Boolean algebra is called *weakly distributive* if whenever $\{D_i\}$ is a sequence of dual ideals with intersection D, the condition $\wedge D_i = 0$ for every i implies $\wedge D = 0$. The following theorem exhibits this condition as a kind of distributive law. By a *multiplicative set* is meant a set that contains $a \wedge b$ whenever it contains a and b.

Theorem 5. *Let A be a Boolean σ-algebra. Let $D_i = \{a_{i,\gamma} : \gamma \in \Gamma_i\}$ be any sequence of non-empty multiplicative sets in A. Let F be the set of all mappings f of the set N of positive integers into $\bigcup \Gamma_i$ such that $f(i) \in \Gamma_i$ for each $i \in N$. In order that the equation*

$$\bigvee_{i \in N} \bigwedge_{\gamma \in \Gamma_i} a_{i,\gamma} = \bigwedge_{f \in F} \bigvee_{i \in N} a_{i,f(i)}$$

hold whenever the left member is defined it is necessary and sufficient that A be weakly distributive.

Proof. Let $\{D_i\}$ be any sequence of dual ideals, with $\wedge D_i = 0$ for each i. Then the left member is defined and equal to 0. Every lower bound of $D = \bigcap D_i$ is less than or equal to $\bigvee_{i \in N} a_{i,f(i)}$, for each $f \in F$. Since $\bigwedge_{f \in F} \bigvee_{i \in N} a_{i,f(i)} = 0$ it follows that $\wedge D$ exists and is equal to 0. Thus the stated law implies that A is weakly distributive.

Now suppose that A is weakly distributive and let $\{D_i\}$ be any sequence of multiplicative sets such that the left member of the equation is defined, say equal to a. For each $i \in N$ define

$$D_i^* = \{(a' \wedge a_{i,\gamma}) \vee c : \gamma \in \Gamma_i,\ c \in A\}.$$

Then D_i^* is a dual ideal in A. If b_i is any lower bound of D_i^* then $b_i \leqq (a' \wedge a_{i,\gamma}) \vee c$ for every $\gamma \in \Gamma_i$ and $c \in A$. In particular, taking $c = a \wedge a_{i,\gamma}$, $b_i \leqq a_{i,\gamma}$ for every $\gamma \in \Gamma_i$. Hence $b_i \leqq \bigwedge_{\gamma \in \Gamma_i} a_{i,\gamma}$, and therefore $b_i \leqq a$. Similarly, taking $c = a' \wedge a'_{i,\gamma}$ we find that $b_i \leqq a'$. Therefore $b_i = 0$. Consequently $\wedge D_i^*$ is defined and equal to 0 for each $i \in N$. It follows that $\wedge D^* = 0$, where $D^* = \bigcap D_i^*$. Let d be any element of D^*. For some $g \in F$ and some sequence $\{c_i\}$ of elements of A we have $d = (a' \wedge a_{i,g(i)}) \vee c_i$ for each $i \in N$. Let b be any lower bound of the set

$$C = \{\bigvee_{i \in N} a_{i,f(i)} : f \in F\}.$$

Then

$$a' \wedge b \leqq a' \wedge \bigvee_{i \in N} a_{i,g(i)} = \bigvee_{i \in N} a' \wedge a_{i,g(i)} \leqq d.$$

Therefore $a' \wedge b \leqq \wedge D^* = 0$, that is, $b \leqq a$. On the other hand,

$$a = \bigvee_{i \in N} \bigwedge_{\gamma \in \Gamma_i} a_{i,\gamma} \leqq \bigvee_{i \in N} a_{i,f(i)}$$

for every $f \in F$, hence a is a lower bound of the set C. Consequently $\wedge C$ exists, is equal to a, and the equation holds under the condition stated.

We remark that in case every disjoint family of non-zero elements of A is countable, this distributive law can be replaced by the requirement that

$$\bigvee_i \bigwedge_j a_{i,j} = \bigwedge_{f \in F} \bigvee_i a_{i,f(i)}$$

for every double sequence $\{a_{i,j}\}$ such that $a_{i,j} \geqq a_{i,j+1}$ for all i and j. In other words, a Boolean σ-algebra that satisfies the countable chain condition is weakly distributive if and only if it is weakly countably distributive in the sense of Horn and Tarski [6, p. 469].

Theorem 6. *If X is a quasi-regular topological space, and if $R(X)$ is weakly distributive, then every set of first category in X is nowhere dense.*

Proof. Let $\{N_i\}$ be any sequence of nowhere dense sets in X, and let $P = \bigcup N_i$. For each i let D_i be the class of all regular open sets that contain N_i. Then D_i is a dual ideal in $R(X)$. Denote the intersection of the sets belonging to D_i by E_i. For any non-empty open set U in X, and for any i, there exists a non-empty open set $V < U - N_i$. Since X is quasi-regular there is a non-empty open set G such that $G^- < V$, and we may assume that G is regular open. Hence $G^{-\prime} > N_i$, $G^{-\prime} \in D_i$, $G^{-\prime} > E_i$, and $G < U - E_i$. This shows that E_i is nowhere dense. Any lower bound of D_i in $R(X)$ is contained in E_i, hence $\bigwedge D_i = 0$ for each i. Let $D = \bigcap_i D_i$. If $G \in D$ then $G > N_i$ for every i, hence $G > P$, and $G > P^{-\prime -\prime}$. Therefore $P^{-\prime -\prime}$ is a lower bound of D in $R(X)$. Since $R(X)$ is weakly distributive, $\bigwedge D = 0$, therefore $P^{-\prime -\prime}$ is empty and P is nowhere dense.

The first example following Theorem 4 shows that Theorem 6 is not true for arbitrary T_1-spaces. In that example $R(X)$ is the 2-element Boolean algebra, which is completely distributive.

The following theorem shows that the converse of Theorem 6 is true for a class of spaces which includes all locally compact Hausdorff spaces. Later (Theorem 17) we shall find that a similar proposition is true for metrizable spaces.

Theorem 7. *Let X be a space with the property that every non-empty open set contains a compact closed set with a non-empty interior. If every set of first category in X is nowhere dense then $R(X)$ is weakly distributive.*

Proof. Let $\{D_i\}$ be any sequence of dual ideals in $R(X)$ with $\bigwedge D_i = 0$ for each i. Let E_i be the intersection of the closures of the sets belonging to D_i. If H is any regular open set contained in E_i and if G is any member of D_i, then $H < G^-$. Since G is regular open it follows that $H < G$. Since $\bigwedge D_i = 0$ we conclude that $H = 0$, therefore E_i is nowhere dense. By hypothesis the set $E = \bigcup E_i$ is also nowhere dense. Let $D = \bigcap_i D_i$ and suppose that $\bigwedge D \neq 0$. Then there exists a compact closed set K with non-empty interior such that K is contained in E' and in every member of D. Hence the interior V of K is a lower bound of D in $R(X)$, and $V^{-\prime} > E_i$ for every i. If the sets of the family $\{G^- \cap K : G \in D_i\}$ were all non-empty, the family would have the finite intersection property and its intersection $E_i \cap K$ would be non-empty, contrary to $K < E'$. Hence $G^- \cap V^- = 0$ and $V^{-\prime} > G$ for some G in D_i. Since $V^{-\prime}$ is regular open it follows that $V^{-\prime} \in D_i$ for every i, therefore $V^{-\prime} \in D$. Hence $V^{-\prime} > K > V$ and $V = 0$. This contradiction shows that $\bigwedge D = 0$, that is, $R(X)$ is weakly distributive.

For the next theorem we shall need the following elementary lemma.

(3.1) *If D is a dual ideal in a measurable Boolean algebra A, and if $\bigwedge D = 0$, then* $\inf \{m(a) : a \in D\} = 0$ *for every measure m in A.*

Proof. Let $\{a_i\}$ be a maximal disjoint family (necessarily countable) of non-zero elements whose complements belong to D. Then $\bigvee a_i = e$ and $\Sigma\, m(a_i) = m(e)$. For any $\varepsilon > 0$ choose n so that $\sum_{i=1}^{n} m(a_i) > m(e) - \varepsilon$. Then $d = \bigwedge_{i=1}^{n} a_i'$ belongs to D and $m(d) = m(e) - m\left(\bigvee_{i=1}^{n} a_i\right) < \varepsilon$.

The following theorem is a slight generalization of a theorem of Horn and Tarski [6, Th. 3. 7].

Theorem 8. *Any measurable Boolean algebra is weakly distributive. More generally, if A is a complete Boolean algebra with unit element e, and if A contains a subset B such that $\bigvee B = e$ and such that for each $b \in B$ the principal ideal $A(b)$ generated by b is measurable, then A is weakly distributive.*

Proof. It suffices to prove the second assertion. Let $\{D_i\}$ be any sequence of dual ideals in A such that $\bigwedge D_i = 0$ for each i. Let $D = \bigcap_i D_i$ and $d = \bigwedge D$. Consider any $b \in B$ and any measure m on $A(b)$. The set $\{a \wedge b : a \in D_i\}$ is a dual ideal $D_i(b)$ in $A(b)$ with $\bigwedge D_i(b) = 0$. By (3. 1), for any $\varepsilon > 0$ and any i there exists an element $a_i \in D_i$ such that $m(a_i \wedge b) \leqq \frac{\varepsilon}{2^i}$. Put $a = \bigvee a_i$. Then $a \in D$ and

$$m(a \wedge b) = m\big(\bigvee (a_i \wedge b)\big) \leqq \Sigma\, m(a_i \wedge b) \leqq \varepsilon.$$

Since $d \leqq a$, $m(d \wedge b) \leqq \varepsilon$ for every $\varepsilon > 0$. Therefore $m(d \wedge b) = 0$ and $d \wedge b = 0$ for every $b \in B$. Consequently

$$d = d \wedge e = d \wedge (\bigvee B) = \bigvee \{d \wedge b : b \in B\} = 0.$$

4. Regularly M-measurable spaces.

Let M be any measurable Boolean algebra. A topological space X will be called *M-measurable* if the category algebra of X is isomorphic to M, and *regularly M-measurable* if X is M-measurable and some category measure in X is regular. In this case every category measure is regular, by Theorem 2.

Theorem 9. *Let M be a measurable Boolean algebra. A topological space X is a regularly M-measurable Baire space if and only if X is quasi-regular and $R(X)$ is isomorphic to M.*

Proof. If X is a regularly M-measurable Baire space, Theorems 1 and 2 show that X is quasi-regular and that $R(X)$ is isomorphic to M. Conversely, if X is quasi-regular and $R(X)$ is isomorphic to M it follows from Theorem 8 that $R(X)$ is weakly distributive, and then from Theorem 6 that X is a Baire space. Hence X is a quasi-regular M-measurable Baire space, therefore a regularly M-measurable Baire space, by Theorem 2.

5. Boolean spaces.

By the Stone representation theorem, corresponding to any Boolean algebra A there is a compact zero-dimensional Hausdorff space X with the property that the algebra $B(X)$ of closed open subsets of X is isomorphic to A. These properties determine X uniquely up to homeomorphism and X is called the Boolean space corresponding to A. It is known that the closure of every open set in X is open if and only if A is complete. This follows from a theorem of Tarski [13, Hilfssatz 6. 7] and also from the following theorem, cf. [5, Th. 37].

Theorem 10. *The following properties of a topological space are equivalent:*

1) *every regular open set in X is closed;*

2) *the closure of every open set in X is open;*

3) *the algebra $B(X)$ of closed open subsets of X is complete, and every non-empty regular open set in X contains a non-empty closed open set.*

Proof. The equivalence of 1) and 2) follows immediately from the inclusions $G < G^{-\prime-\prime} < G^{-}$. Assume 2) and let G be the closure of the union of any family $\mathscr{F}$ of closed open sets. Then G is the least upper bound of $\mathscr{F}$ in $B(X)$. The second part of 3) follows trivially from 1). Hence 2) implies 3).

Now assume 3) and let U be any open set in X. Let G be the least upper bound in $B(X)$ of the family $\mathscr{F}$ of all closed open sets contained in $U^{-\prime-\prime}$. If H is any closed open set contained in $U^{-\prime-\prime} \cap G'$ then $H \in \mathscr{F}$, hence $H < G \cap G' = 0$. Since $U^{-\prime-\prime} \cap G'$ is regular open it follows from 3) that it must be empty, hence $U^{-\prime-\prime} < G$.

Similarly, if H is any closed open set contained in $G \cap U^{-\prime}$ then $H' > U^{-} > J$ for every J in $\mathscr{F}$. Hence $H' > G$ and therefore $H < G' \cap G = 0$. Since $G \cap U^{-\prime}$ is regular open it follows again from 3) that $G \cap U^{-\prime} = 0$, that is, $G < U^{-}$.

Having shown that $U < U^{-\prime-\prime} < G < U^{-}$ we conclude that $U^{-} = G$. Thus 3) implies 2).

Corollary. *A zero-dimensional space X has property* 1) *or* 2) *if and only if $B(X)$ is complete.*

Following Dixmier [4] we shall call the Boolean space corresponding to a complete Boolean algebra a *Stonian space.* Since any Hausdorff space that satisfies 2) is totally disconnected we see that a compact Hausdorff space X is Stonian if and only if it satisfies 2), or equivalently, if and only if it is extremally disconnected in the sense of Hewitt [5].

Theorem 11. *A compact Boolean space X has the property that every set of first category in X is nowhere dense if and only if $B(X)$ is weakly distributive*[1]).

Proof. We shall show that $B(X)$ is weakly distributive if and only if $R(X)$ is. Then the conclusion follows from Theorems 6 and 7. For any dual ideal D in $R(X)$ let D^* be the class of closed open sets that belong to D. Then D^* is a dual ideal in $B(X)$. If D_1 is any dual ideal in $B(X)$ let D be the class of all regular open supersets of members of D_1. Then D is a dual ideal in $R(X)$ and $D^* = D_1$. Thus the correspondence $D \to D^*$ is a mapping of the class of dual ideals in $R(X)$ onto the class of dual ideals in $B(X)$. Let us denote greatest lower bounds in $R(X)$ by $\wedge$, and in $B(X)$ by $\wedge^*$. If D is a dual ideal in $R(X)$, and if $G \in D$, then G^{-} is the intersection of the family of closed open sets that contain G. Since this family is contained in D^* it follows that any lower bound B of D^* in $B(X)$ is contained in G^{-}, and therefore in G since G is regular open. Therefore $\wedge D = 0$ implies $\wedge^* D^* = 0$. On the other hand, if $\wedge D \neq 0$ there exists a non-empty closed open set $B < \wedge D$. Then B is contained in every member of D^*, hence $\wedge^* D^* \neq 0$. Thus $\wedge D = 0$ if and only if $\wedge^* D^* = 0$.

Let $\{D_i\}$ be any sequence of dual ideals in $R(X)$. Then $\{D_i^*\}$ is a sequence of dual ideals in $B(X)$, and any sequence of dual ideals in $B(X)$ can be so represented. If

[1]) For complete Boolean algebras that satisfy the countable chain condition, *J. L. Kelley* [Pacific J. Math 1 (1959), 1165-1177] has obtained an equivalent result, with „weakly countably distributive" in place of „weakly distributive". By considering the one-point compactification of an infinite discrete space it may be seen, that the present theorem is somewhat wider in scope.

$D = \bigcap_i D_i$ then $D^* = \bigcap_i D_i^*$. Since $\wedge D_i = 0$ if and only if $\wedge^* D_i^* = 0$, and $\wedge D = 0$ if and only if $\wedge^* D^* = 0$, it follows that $R(X)$ is weakly distributive if and only if $B(X)$ is weakly distributive.

An example due to Dieudonné [4, p. 30] shows that in a Stonian space it may happen that every set of first category is nowhere dense while at the same time every Borel measure has a nowhere dense support. It follows that a Boolean algebra can be complete and weakly distributive without being measurable even in the weak sense demanded in Theorem 8.

6. Maps in Boolean spaces.

Let M be any given measurable Boolean algebra. We now consider the problem of constructing all regularly M-measurable Baire spaces. By Theorem 9 this is equivalent to constructing all quasi-regular spaces whose regular algebra is isomorphic to M.

Since M is complete, the Boolean space Y corresponding to M is Stonian. By Theorem 10, $R(Y) = B(Y)$ and therefore $R(Y)$ is isomorphic to M. Since any compact Hausdorff space is quasi-regular we see that Y is one example of a regularly M-measurable Baire space (cf. [4], [8], [9]). To find all such spaces it is natural to apply Stone's theory of maps in Boolean spaces. In fact, Stone has already proposed the problem of determining all the different T_0-spaces whose regular algebra is isomorphic to a given complete Boolean algebra, and has expressed the opinion that paper [10] "provides methods which should suffice for a deep investigation, if not actually for a complete solution, of this problem" [12, p. 262]. We shall show that an appropriate specialization of Stone's construction does indeed provide a solution of this problem, and that a further specialization leads to a determination of all regularly M-measurable Baire spaces.

Let Z be a topological space. Let f be a mapping of a set X onto a class $\mathcal{F}$ of non-empty subsets of Z. For each open set G in Z define $X(G) = \{x : f(x) < G\}$. Then $X(G \cap H) = X(G) \cap X(H)$ and $X(Z) = X$. Hence the class of sets $\{X(G) : G$ open in $Z\}$ constitute a base for a topology in X. We call this the topology induced in X by f and Z. It is obvious that X can be a T_0-space only if f is one-to-one. In case Z is a T_1-space this condition is also sufficient. For if there is a point z in $f(x_2) - f(x_1)$ then $G = Z - \{z\}$ is an open subset of Z such that $x_1 \in X(G)$ and $x_2 \notin X(G)$.

Theorem 12. *Let Z be a topological space and let Y be a closed subset of Z. Let $\mathcal{F}$ be a family of subsets of Z such that*

(1) *each member of $\mathcal{F}$ meets Y, and*

(2) *any open set in Z that meets Y contains at least one member of $\mathcal{F}$.*

Let f be a mapping of a set X onto $\mathcal{F}$. Under the topology induced in X by f and Z the regular algebra of X is isomorphic to the regular algebra of Y. If Y is a quasi-regular subspace of Z then X is quasi-regular if and only if $\mathcal{F}$ satisfies the further condition:

(3) *for any open set G that meets Y there is an open set H that meets Y and is such that G contains every member of $\mathcal{F}$ that meets $H \cap Y$.*

The *proof* consists of a series of lemmas leading to (6. 9) and (6. 10).

(6. 1) *If G is open in Z then*

$$X^-(G) = \{x : f(x) \cap (G \cap Y)^- \neq 0\}.$$

Proof. Suppose $f(x) \cap (G \cap Y)^- \neq 0$. Let $X(H)$, H open in Z, be any basic open set containing x. Then $f(x) < H$ and

$$H \cap (G \cap Y)^- > f(x) \cap (G \cap Y)^- \neq 0.$$

Since H is open it follows that $H \cap G \cap Y \neq 0$. By (2) there exists a point $x_0 \in X$ such that $f(x_0) < H \cap G$. Hence $X(H) \cap X(G) = X(H \cap G)$ is non-empty. Therefore $x \in X^-(G)$.

Suppose $f(x) \cap (G \cap Y)^- = 0$. Put $H = (G \cap Y)^{-\prime}$. Then H is an open set containing $f(x)$, and $H \cap G \cap Y = 0$. It follows from (1) that $X(H \cap G) = 0$. Therefore $X(H)$ is an open set containing x and disjoint to $X(G)$. Hence $x \notin X^-(G)$.

(6. 2) *If G is open in Z then*

$$X^{-\prime -\prime}(G) = X(K \cup Y'),$$

where K is the smallest member of $R(Y)$ that contains $G \cap Y$.

Proof. By (6. 1), $X^{-\prime}(G) = X\big((G \cap Y)^{-\prime}\big)$. A second application of this formula shows that $X^{-\prime -\prime}(G) = X(H)$, where $H = \big((G \cap Y)^{-\prime} \cap Y\big)^{-\prime}$. The Y-complement of the Y-closure of any subset E of Y is

$$(E^- \cap Y)' \cap Y = E^{-\prime} \cap Y.$$

Hence the Y-interior of the Y-closure of E (that is, the smallest member of $R(Y)$ containing E) is the set $F = (E^{-\prime} \cap Y)^{-\prime} \cap Y$. Therefore

$$F \cup Y' = (E^{-\prime} \cap Y)^{-\prime} \cup Y' = (E^{-\prime} \cap Y)^{-\prime}.$$

In particular, if $E = G \cap Y$ then $F = K$, and we conclude that $K \cup Y' = H$.

(6. 3) *If J is open relative to Y then $J \cup Y'$ is open in Z.*

Proof. $J = G \cap Y$ for some set G open in Z. Hence

$$J \cup Y' = (G \cap Y) \cup Y' = G \cup Y'.$$

Since both G and Y' are open in Z so is $J \cup Y'$.

(6. 4) *If $J \in R(Y)$ and $K = Y - J^-$ then*

$$X^{-\prime}(J \cup Y') = X(K \cup Y').$$

Proof. By (6. 1) and (6. 3),

$$X^{-\prime}(J \cup Y') = \{x : f(x) \cap \big((J \cup Y') \cap Y\big)^- = 0\} = X(J^{-\prime}).$$

Since

$$K \cup Y' = (J^{-\prime} \cap Y) \cup Y' = J^{-\prime} \cup Y' = J^{-\prime}$$

the conclusion follows.

(6. 5) *If $J \in R(Y)$ then*

$$X^{-\prime -\prime}(J \cup Y') = X(J \cup Y').$$

Proof. Let $K = Y - J^-$. Then $K \in R(Y)$ and $J = Y - K^-$, since J is regular open relative to Y. Two applications of (6. 4) give the conclusion.

(6. 6) *If J and K belong to $R(Y)$ then*

$$X\big((J \cap K) \cup Y'\big) = X(J \cup Y') \cap X(K \cup Y').$$

Proof. Apply the distributive law.

(6. 7) *If $J \in R(Y)$ and $J \neq 0$ then*

$$X(J \cup Y') \neq 0.$$

Proof. Let $J = G \cap Y$, G open in Z. Since G meets Y, (2) implies that $X(G) \neq 0$. Since

$$J \cup Y' = (G \cap Y) \cup Y' = G \cup Y' > G$$

it follows that $X(J \cup Y') \neq 0$.

(6. 8) *If H is any regular open subset of X then $H = X(J \cup Y')$ for some $J \in R(Y)$.*

Proof. Let $\mathcal{K}$ be the class of all sets $K \in R(Y)$ such that $X(K \cup Y') \subset H$. Let U be the union of the sets belonging to $\mathcal{K}$ and let J be the smallest member of $R(Y)$ containing U. Since H is open, for each $x \in H$ there is a basic open set $X(G)$, G open in Z, such that $x \in X(G) \subset H$. Hence $x \in X^{-\prime-\prime}(G) \subset H$. From (6. 2) it follows that $x \in X(K \cup Y') \subset H$ for some $K \in R(Y)$. Hence $K \in \mathcal{K}$ and $K \subset J$. Therefore

$$f(x) \subset K \cup Y' \subset J \cup Y'$$

and we conclude that $H \subset X(J \cup Y')$.

Now consider any $x \in X(J \cup Y')$. Let $X(G)$, G open in Z, be any basic open set containing x. Then $f(x) \subset G \cap (J \cup Y')$. By (1) there is a point $y \in f(x) \cap Y$. Hence $y \in G \cap J$. Since $J \subset U^-$ it follows that $G \cap U^- \neq 0$ and therefore $G \cap U \neq 0$. Hence $G \cap K \neq 0$ for some $K \in \mathcal{K}$. Therefore, by (6. 3), $G \cap (K \cup Y')$ is an open set in Z that meets Y. By (2) there exists a point $x_0 \in X$ such that $f(x_0) \subset G \cap (K \cup Y')$. Hence $x_0 \in X(G)$ and $x_0 \in X(K \cup Y') \subset H$. Therefore $X(G) \cap H \neq 0$. It follows that $x \in H^-$ and we conclude that $X(J \cup Y') \subset H^-$.

From the relations $H \subset X(J \cup Y') \subset H^-$ and $H = H^{-\prime-\prime}$ it follows that

$$H = X^{-\prime-\prime}(J \cup Y') = X(J \cup Y'),$$

by (6. 5).

(6. 9) *The correspondence $J \to X(J \cup Y')$ is an isomorphism of $R(Y)$ onto $R(X)$.*

Proof. By (6. 5) and (6. 8) this correspondence is a mapping of $R(Y)$ onto $R(X)$. By (6. 4) and (6. 6) it is a homomorphism, and by (6. 7) it is an isomorphism.

(6. 10) *In order that X be quasi-regular it is necessary that $\mathcal{F}$ satisfy condition* (3). *This condition is sufficient in case Y is quasi-regular.*

Proof. Suppose X is quasi-regular. Let G be any open set that meets Y. Then $X(G)$ is non-empty and there exists a non-empty open set V such that $V^- \subset X(G)$. Let $X(H)$ be a non-empty basic open subset of V. Then H is open in Z, H meets Y, and if $f(x) \cap H \cap Y \neq 0$ then $f(x) \cap (H \cap Y)^- \neq 0$ and $x \in X^-(H)$, by (6. 1). Hence $x \in V^- \subset X(G)$ and $f(x) \subset G$. Therefore $\mathcal{F}$ satisfies (3).

Suppose $\mathcal{F}$ satisfies (3) and Y is quasi-regular. Any non-empty open set in X contains a non-empty basic open set $X(G)$. Then G meets Y. By (3) there exists an open set H_1 that meets Y and is such that $f(x) \cap H_1 \cap Y \neq 0$ implies $f(x) \subset G$. Since Y is quasi-regular there exists an open set H such that $H \cap Y \neq 0$ and $(H \cap Y)^-$ (which is also the closure of $H \cap Y$ relative to Y) is contained in $H_1 \cap Y$. Then $X(H)$ is a non-empty open set, and if $x \in X^-(H)$ then $f(x) \cap (H \cap Y)^- \neq 0$, $f(x) \cap H_1 \cap Y \neq 0$, $f(x) \subset G$, and $x \in X(G)$. Therefore $X^-(H) \subset X(G)$ and X is quasi-regular.

We call attention to the following corollary of Theorem 12.

(6. 11) *If X is a dense subspace of a topological space Y, then $R(X)$ is isomorphic to $R(Y)$. If Y is quasi-regular then so is X.*

Concerning conditions (1) and (2) of Theorem 12 we make the following comment. To any family $\mathcal{F}$ of subsets of Z can be associated the set Y^* consisting of all points of Z with the property that every neighborhood of z contains at least one member of $\mathcal{F}$. Y^* is a closed set. If $\mathcal{F}$ satisfies (1) and (2) then $Y = Y^*$. In any case (2) is satisfied when $Y = Y^*$. Hence the restriction imposed upon $\mathcal{F}$ by conditions (1) and (2) is simply that each member of $\mathcal{F}$ should intersect the associated set Y^*.

7. Algebraic maps in Boolean spaces.

We now consider a representation of an arbitrary T_0-space X by a map of the kind described in Theorem 12. The map defined in the following theorem was introduced by Stone and is called an *algebraic map* of X [10, Th. 26].

Theorem 13. *Let X be an arbitrary T_0-space. Let $\mathbf{B}$ be a subring of the complete basic ring of X that includes a base and includes all regular open sets. Let Z be the Boolean space corresponding to $\mathbf{B}$, and let g be an isomorphism of $\mathbf{B}$ onto $B(Z)$. Let $\mathbf{N}$ be the class of nowhere dense sets that belong to $\mathbf{B}$, and let Z_0 be the union of the sets $g(N)$ for $N \in \mathbf{N}$. For each x in X let*

$$\mathbf{B}(x) = \{B : B \in \mathbf{B},\ x \in B'^{-\prime}\}$$

and let $f(x)$ be the intersection of the family $\{g(B) : B \in \mathbf{B}(x)\}$. Then

(i) *the set $Y = Z - Z_0$ is a Stonian subspace of Z and $R(X)$ is isomorphic to $R(Y)$,*

(ii) *the class $\mathcal{F} = \{f(x) : x \in X\}$ is a family of closed subsets of Z that satisfies conditions* (1) *and* (2) *of Theorem* 12 *relative to Y,*

(iii) *f is a one-to-one mapping of X onto $\mathcal{F}$, and*

(iv) *the topology induced in X by f and Z is identical with the given topology in X.*

In case X is quasi-regular the family $\mathcal{F}$ satisfies a condition stronger than (3), *namely,*

(3′) *for any open set G that meets Y there is an open set H that meets Y and is such that G contains every member of $\mathcal{F}$ that meets H.*

Proof. All but the last assertion of this theorem are included in or implied by Theorems 4 (4), 26, and 28 of [10]. Accordingly we shall give the proof in somewhat condensed form. Observe first that for each $x \in X$, $\mathbf{B}(x)$ is a dual ideal in $\mathbf{B}$ and that $f(x)$ is the intersection of a family of closed open sets, hence closed.

(7. 1) *If $B \in \mathbf{B}$ then $g(B) \subset Z_0$ if and only if $B \in \mathbf{N}$.*

If $g(B) \subset Z_0$ then $g(B)$ can be covered by a finite number of sets $g(N_i)$ with $N_i \in \mathbf{N}$, hence $B \in \mathbf{N}$. The converse is true by definition.

(7. 2) *$f(x) \cap Y \neq 0$ for each $x \in X$.*

This follows from the fact that $g(\mathbf{B}(x)) \cap Y$ is a family of sets having the finite intersection property.

(7. 3) *If $B \in \mathbf{B}$ then $f(x) \subset g(B)$ if and only if $x \in B'^{-\prime}$.*

If the sets of the family $g(\mathbf{B}(x))$ all met $Z - g(B)$ then so would $f(x)$. Hence $f(x) \subset g(B)$ implies $f(x) \subset g(A) \subset g(B)$ for some $A \in \mathbf{B}(x)$, and therefore $x \in A'^{-\prime} \subset B'^{-\prime}$. The converse is true by definition.

(7. 4) *If $B \in \mathbf{B}$ then $f(x) \cap g(B) \neq 0$ if and only if $x \in B^{-}$.*

Replace B by B' in (7. 3).

(7. 5) *The mapping $B \to h(B) = g(B) \cap Y$ is a homomorphism of $\mathbf{B}$ onto $B(Y)$, and the kernel of h is $\mathbf{N}$.*

Any member of $B(Z)$ intersects Y in a set that is closed open relative to Y, and every member of $B(Y)$ can be so represented. Hence h maps $\mathbf{B}$ onto $B(Y)$. It is then easy to verify that h is a homomorphism, and (7. 1) shows that the kernel of h is $\mathbf{N}$.

By (7. 5) Y is the Boolean space corresponding to $\mathbf{B}/\mathbf{N}$. Since $\mathbf{B}$ includes all regular open sets it follows that $B(Y)$ is isomorphic to $R(X)$. By Theorem 10, Y is Stonian and $R(Y) = B(Y)$. Thus assertion (i) is proved. That $\mathcal{F}$ satisfies conditions (1) and (2) follows

from (7. 2), (7. 1), and (7. 3). Assertion (iii) follows from the fact that if x_1 and x_2 are any two distinct points of X there is an open set $B \in \boldsymbol{B}$ that contains one but not both. Hence, by (7. 3), $g(B)$ contains one but not both of the sets $f(x_1)$ and $f(x_2)$. (7. 3) also shows that the topology induced in X has for base the family of sets $\{B'^{-\prime} : B \in \boldsymbol{B}\}$. It is therefore identical with the given topology. It only remains to prove the following lemma.

(7. 6) *If X is quasi-regular then $\mathscr{F}$ satisfies condition* (3′).

It suffices to consider any closed open set $G = g(B)$ that meets Y. Then $B'^{-\prime}$ is a non-empty open set in X, by (7. 1). Since X is quasi-regular and $\boldsymbol{B}$ includes a base there exists a non-empty open set $A \in \boldsymbol{B}$ such that $A^- \subset B'^{-\prime}$. Take $H = g(A)$. Then (7. 1) shows that H meets Y, and (7. 4) shows that if $f(x)$ meets H then $x \in A^-$, hence $x \in B'^{-\prime}$ and $f(x) \subset g(B)$. Thus G contains every member of $\mathscr{F}$ that meets H.

Theorems 12 and 13 justify the following construction. Let A be a complete Boolean algebra, and let Y be the corresponding Boolean space. Then $R(Y)$ is isomorphic to A. Let Z be any compact Boolean space in which Y can be imbedded, let $\mathscr{F}$ be a family of closed subsets of Z that satisfies conditions (1) and (2) of Theorem 12 relative to some imbedding of Y in Z, and let f be a one-to-one mapping of a set X onto $\mathscr{F}$. According to Theorem 12 the topology induced in X by f and Z makes X a T_0-space whose regular algebra is isomorphic to A. Theorem 13 shows that by an appropriate choice of Z and $\mathscr{F}$ every such space can be so obtained. By relaxing the requirement that f be one-to-one we can obtain in this way all topological spaces whose regular algebra is isomorphic to A, since it is known, [11], [3], that any topological space can be mapped onto a T_0-space by a mapping that induces a one-to-one correspondence between their families of open sets, and therefore an isomorphism between their regular algebras.

In the above construction we may confine attention to Boolean spaces Z of a special class, and to a particular imbedding of Y in each. Let c be any infinite cardinal number not less than that of A. Let Z_c be the topological product of a family $\{Z_\alpha : \alpha \in I\}$ of replicas of the 2-point space $Z_\alpha = \{0, 1\}$, where I is an index set of power c. Stone has shown [10, Th. 10] that every Boolean space of character not exceeding c can be imbedded in Z_c. We need to consider a slightly specialized form of this imbedding.

Let φ be a mapping of I onto $B(Y)$ such that each of the sets $\varphi^{-1}(G)$, $G \in B(Y)$, has power c. For each $y \in Y$ let $g(y)$ be the point $\{z_\alpha\}$ of Z_c defined by taking $z_\alpha = 1$ if $y \in \varphi(\alpha)$ and $z_\alpha = 0$ if $y \notin \varphi(\alpha)$. Then g is a homeomorphism of Y onto a subspace Y_0 of Z_c. Let us call Y_0 a *suitable* imbedding of Y in Z_c. Suppose that we are also given an imbedding of Y in a space Z such that $B(Z)$ has power not exceeding c. Let ψ be a mapping of I onto $B(Z)$ such that $\psi(\alpha) \cap Y = \varphi(\alpha)$ for each $\alpha \in I$. Such a mapping exists since at least one and at most c members of $B(Z)$ intersect Y in any specified set belonging to $B(Y)$. For each $z \in Z$ let $h(z)$ be the point $\{z_\alpha\}$ of Z_c defined by taking $z_\alpha = 1$ if $z \in \psi(\alpha)$ and $z_\alpha = 0$ if $z \notin \psi(\alpha)$. Then h is a homeomorphism of Z onto a subspace Z_0 of Z_c, and h is an extension of g. It follows from Theorem 13 that any T_0-space whose regular algebra is isomorphic to A and which has a ring $\boldsymbol{B}$ (as in Theorem 13) with power not exceeding c can be represented by a family $\mathscr{F}$ of closed subsets of Z_0 (therefore also closed in Z_c) that has properties (1) and (2) relative to Y_0. The topology induced by Z_c is the same as that induced by Z_0. On the other hand, any space X represented by a family of subsets of Z_c has character not exceeding c. Hence we have the following theorem.

Theorem 14. *Let A be a complete Boolean algebra, and let Y be the corresponding Boolean space. Let c be any infinite cardinal number not less than that of A. Let Y_0 be a suitable imbedding of Y in Z_c. Let $\mathscr{F}$ be a family of closed subsets of Z_c that satisfies conditions*

(1) and (2) of Theorem 12 relative to Y_0, and let f be a one-to-one mapping of a set X onto $\mathcal{F}$. The topology induced in X by f and Z_c makes X a T_0-space of character not exceeding c whose regular algebra is isomorphic to A. Any T_0-space whose complete basic ring (or some ring that includes a base and all regular open sets) has power not exceeding c and whose regular algebra is isomorphic to A corresponds in this way to some such family $\mathcal{F}$. X is quasi-regular if and only if $\mathcal{F}$ also satisfies condition (3).

In particular, if M is any measurable Boolean algebra then all regularly M-measurable Baire T_0-spaces can be constructed by suitably imbedding the Boolean space Y corresponding to M in each of the spaces Z_c, $c \geqq$ power of M, and then choosing families of closed subsets of Z_c that satisfy conditions (1), (2), and (3) of Theorem 12 relative to this imbedding of Y.

8. Specializations.

The construction described in Theorem 14 gives rise to a T_0-space X. X is a T_1-space if and only if no member of $\mathcal{F}$ contains another, and a Hausdorff space if the members of $\mathcal{F}$ are mutually disjoint [10, Th. 23].

In Theorem 14 no bound can in general be placed upon c, as the following example shows. Let X be an arbitrary infinite set, and let D be a denumerable subset of X. Topologize X by taking for open sets all subsets of D and all subsets of X that contain all but a finite number of points of D. Then X is a T_1-space containing D as a dense subset. Each point of D is an isolated point of X, hence X is quasi-regular and every nowhere dense set is contained in $X - D$. On the other hand, every subset of $X - D$ is a nowhere dense closed set. Hence the complete basic ring of X is the field of all subsets of X. Its quotient modulo nowhere dense sets is isomorphic to the field of all subsets of D, and therefore to the measure algebra M of an infinite discrete measure space. Hence X is a regularly M-measurable Baire T_1-space. A family of subsets of X is a base if and only if it includes each one-element subset of D and for each $x \in X - D$ a sequence of sets of the form $\{x\} \cup (D - F_i)$, where $\{F_i\}$ is a generating sequence for the ideal of finite subsets of D. The character of X is therefore equal to the power of X, which may be taken arbitrarily large.

However, if we confine attention to *Hausdorff* spaces then a single choice of Z_c is sufficient, as we now show. Write $\exp r = 2^r$ for any cardinal number r.

Theorem 15. *Let A be a complete Boolean algebra, with cardinal number r. Let $c = \exp \exp r$, and let Y_0 be a suitable imbedding of the Boolean space corresponding to A in Z_c. Let $\mathcal{F}$ be any family of mutually disjoint closed subsets of Z_c that satisfies conditions (1) and (2) of Theorem 12 relative to Y_0. Let f be a one-te-one mapping of a set X onto $\mathcal{F}$. The topology induced in X by f and Z_c makes X a Hausdorff space whose regular algebra is isomorphic to A. Every such space can be so represented.*

Proof. The first assertion follows from Theorem 14 and the remark that X is Hausdorff whenever $\mathcal{F}$ is a disjoint family of closed sets. To prove the other assertion, let X be any Hausdorff space with $R(X)$ isomorphic to A. Let b be the cardinal number of the complete basic ring $\boldsymbol{B}$ of X, and let f be the algebraic map of X in the Boolean space Z corresponding to $\boldsymbol{B}$ defined in Theorem 13. By (7. 3), the range of f is a family of mutually disjoint subsets of Z. By Theorem 13, each of these meets the Stonian subspace Y there defined. Hence the power of X does not exceed that of Y. Because $R(X)$ is isomorphic to $R(Y)$, and $R(Y) = B(Y)$, it follows that Y is the Boolean space corresponding to A,

hence its power does not exceed $\exp r$. Consequently, $b \leqq \exp \exp r$. The conclusion then follows from Theorem 14.

Let us now consider the effect of taking $\mathcal{F}$ to be a family of subsets of the Boolean space Y corresponding to A. The construction described in Theorem 12 can then be carried out entirely within Y. A family of non-empty sets is said to be *densely distributed* in a space if every non-empty open set contains at least one member of the family. If we take $Z = Y$ in Theorem 12, conditions (1) and (2) reduce to the assertion that $\mathcal{F}$ is densely distributed in Y. In case $Y = Z$ is semi-regular (in particular, if it is a Boolean space) it follows from (6. 9) that X is also semi-regular, cf. [10, Th. 62]. For semi-regular spaces the following simpler representation can be used in place of Theorem 13.

(8. 1) *Let X be a semi-regular T_0-space, let Y be the Boolean space corresponding to $R(X)$, and let g be an isomorphism of $R(X)$ onto $B(Y)$. For each x in X let $f(x)$ be the intersection of the family $\{g(B) : x \in B \in R(X)\}$. Then the family $\mathcal{F} = \{f(x) : x \in X\}$ is densely distributed in Y, f is a one-to-one mapping of X onto $\mathcal{F}$, and the topology induced in X by f and Y is identical with the given topology in X.*

All of these assertions follow easily from the fact that $f(x) < g(B)$ if and only if $x \in B$ (cf. (7. 3)). Thus we have the following theorem.

Theorem 16. *Let Y be the Boolean space corresponding to a complete Boolean algebra A. Let $\mathcal{F}$ be any family of non-empty closed sets densely distributed in Y, and let f be a one-to-one mapping of a set X onto $\mathcal{F}$. The topology induced in X by f and Y makes X a semi-regular T_0-space with $R(X)$ isomorphic to A. Any semi-regular T_0-space whose regular algebra is isomorphic to A can be so represented. In order that X be quasi-regular it is necessary and sufficient that $\mathcal{F}$ have the additional property that for every closed open set $G \neq 0$ in Y there exists a closed open set $H \neq 0$ such that G contains every member of $\mathcal{F}$ that meets H.*

When $\mathcal{F}$ is taken to be a *continuous family* [10, Def. 5] the space X is regular. Conversely, when X is regular the map defined in (8. 1) represents X by a continuous family. When $\mathcal{F}$ is a continuous family that covers Y then X is compact. Conversely, when X is compact the family $\mathcal{F}$ defined by (8. 1) covers Y. Thus compact Hausdorff (resp. regular) spaces X such that $R(X)$ is isomorphic to A are characterized as those spaces that can be represented as a continuous image of Y (resp. a subspace of Y) by a mapping h such that the family $\{h^{-1}(x) : x \in X\}$ is densely distributed in Y.

By (6. 11), if X is a compact Hausdorff space with $R(X)$ isomorphic to A then any dense subspace Q of X is a completely regular space and $R(Q)$ is isomorphic to A. Every such space can be so obtained, since X may be taken to be the Stone-Čech compactification of Q. The completely regular spaces whose regular algebra is isomorphic to A are therefore characterized as those spaces which can be represented by a densely distributed family in Y that can be imbedded in a continuous covering family, cf. [10, Th. 92].

9. Metrizable spaces.

The M-measurable spaces we have just constructed are not in general metrizable. In fact, a metrizable Baire space can be M-measurable only if M is of a very special type, namely, isomorphic to the field of all subsets of a countable set.

It follows from Theorem 3 that in any metrizable measurable Baire space every set of first category must be nowhere dense. Let us first determine what restriction is imposed by this requirement alone.

Theorem 17. *The following properties of a metric space X are equivalent:*

1) *every set of first category in X is nowhere dense;*

2) *the set D of isolated points of X is dense in X;*

3) *$R(X)$ is isomorphic to the field of all subsets of some set;*

4) *$R(X)$ is complete and completely distributive;*

5) *$R(X)$ is weakly distributive.*

Proof. Suppose the open set $X - D^-$ is non-empty. For each positive integer n let E_n be a maximal subset of $X - D^-$ with the property that the distance between any two points of E_n is at least equal to $\frac{1}{n}$. Then E_n is closed. Since $X - D^-$ contains no isolated points, each of the sets E_n is nowhere dense. Hence the set $P = \bigcup E_n$ is of first category in X. The maximality of the sets E_n implies that P is dense in $X - D^-$. Hence $X - D^-$ is a non-empty open set contained in P^-, and P is not nowhere dense. Since this contradicts 1) it follows that 1) implies 2). (In case D is empty, the same reasoning shows that a metric space contains a dense set of first category if and only if the space is dense in itself.)

If the set D of isolated points of X is dense in X, then the nowhere dense sets are the subsets of $X - D$, and the complete basic ring is the field of all subsets of X. The mapping $E \to E \cap D$ is a homomorphism of this field onto the field of all subsets of D. Since the kernel of this homomorphism is the ideal of nowhere dense sets it follows that $R(X)$ is isomorphic to the field of all subsets of D. Thus 2) implies 3).

Obviously 3) implies 4). Theorem 5 shows that 4) implies 5); and 5) implies 1) by Theorem 6.

The following conclusion follows from Theorems 3 and 17.

Theorem 18. *A metrizable space is a measurable Baire space if and only if the set D of isolated points of X is a countable dense subset of X. In this case the category measures in X are those and only those measures that are positive for each point of D and vanish on $X - D$.*

Bibliography.

[1] *P. Alexandroff* and *H. Hopf*, Topologie I, Berlin 1935.

[2] *G. Birkhoff*, Lattice theory, 2nd ed., New York 1948.

[3] *E. Čech*, On bicompact spaces, Ann. of Math. (2) **38** (1937), 823—844.

[4] *J. Dixmier*, Sur certains espaces considérés par M. H. Stone, Summa Brasil. Math. **2** (1951), 151—182.

[5] *E. Hewitt*, A problem of set-theoretic topology, Duke Journ. Math. **10** (1943), 309—333.

[6] *A. Horn* and *A. Tarski*, Measures in Boolean algebras, Trans. Amer. Math. Soc. **64** (1948), 467—497.

[7] *C. Kuratowski*, Topologie I, 4th ed., Warsaw 1958.

[8] *E. Marczewski* and *R. Sikorski*, Remarks on measure and category. Coll. Math. **2** (1949), 13—19.

[9] *Y. Mibu*, Relations between measure and topology in some Boolean space, Proc. Imp. Acad. Tokyo **20** (1944), 454—458.

[10] *M. H. Stone*, Applications of the theory of Boolean rings to general topology, Trans. Amer. Math. Soc. **41** (1937), 375—481.

[11] *M. H. Stone*, Applications of Boolean algebras to topology, Mat. Sbornik N. S. **1** (1936), 765—772.

[12] *M. H. Stone*, Algebraic characterizations of special Boolean rings, Fund. Math. **29** (1937), 223—303.

[13] *A. Tarski*, Ideale in vollständigen Mengenkörpern, II, Fund. Math. **33** (1939), 51—65.

Eingegangen 2. Dezember 1959.

On the Reducibility of Certain Linear Differential Systems.

By *Michael Golomb* at Lafayette (Ind.), U.S.A.

0. Introduction.

In this paper systems of the form

$$\frac{dw}{dz} = A_0 w + \lambda A(z)\, w \tag{0. 1}$$

are considered, where the independent variable z and the parameter λ are real or complex, and the variable coefficients which are the components of the matrix $A(z)$ are elements of a class $\mathfrak{P}(\Omega, \mathfrak{B})$. The functions of this class have exponential expansions with exponents from the set Ω, convergent uniformly and absolutely in the part $\mathfrak{B}$ of the complex plane (for a precise definition see Section 1). A principal result is that such systems have fundamental solutions of the form $U(z) \exp(Tz)$, where T is a constant matrix that converges to A_0 as $\lambda \to 0$ and the components of $U(z)$ are functions in $\mathfrak{P}(\Omega_0, \mathfrak{B})$, Ω_0 being the set obtained from Ω by forming all finite linear combinations with nonnegative integral coefficients (Theorem 2. 1). If the substitution $w = Uv$ is made system (0. 1) becomes $\frac{dv}{dz} = Tv$, thus is reduced to a system with constant coefficients by a nonsingular transformation U, which together with its inverse U^{-1} are of class $\mathfrak{P}(\Omega_0, \mathfrak{B})$. This "reducibility $\mathfrak{P}(\Omega_0, \mathfrak{B})$", which is well known for systems with periodic coefficients (Floquet's Theory, [3]) is proved here for the far more general systems (0. 1) (Section 3).

The one essential condition which makes the convergence proof for the given expansions possible is that the set Ω_0 does not have 0 as a limit point. Other restrictions on the characteristic values of the matrix A_0 and on the parameter λ are inessential and can be obviated by modified expansion procedures, especially in certain important particular cases (Section 4). The method by which the expansions of the solution (which are not expansions in powers of λ) are obtained and by which their convergence is proved is essentially that developed by Wasow [14] and Golomb [4, 5] in connection with the study of periodic solutions and stability problems for linear and nonlinear systems. The formal procedure involved had been suggested by E. Weber (see Wasow ([14]).

The expansions on which the proofs for the structure theorems are based are of interest in themselves, as they provide explicit solution procedures. For systems with periodic coefficients, where Floquet's theory gives only existence and structure theorems, this method gives novel series expansions for the solution (see Golomb [5], where this is carried out in detail for Mathieu's and Hill's equations; for other convergent expansions in the periodic case see Lindstedt [8], Poincaré [10], Picard [9], Cesari [1], Hale [6], Sibuya [12, 13]). In this paper the same procedure is applied to obtain convergent series expansions for the solution of linear systems in the neighborhood of an irregular singular point. This appears as a special case of the general theory presented here, by letting Ω_0 be the set of rational integers and replacing the independent variable in equation (0. 1) by $\zeta = \exp z$ (Section 5).

1. The Class of Coefficient Functions.

The class of functions f considered here are complex-valued and defined in a part $\mathfrak{B}$ of the complex z-plane which contains at least two points. They are assumed to have exponential expansions

$$f(z) = \sum_k a_k e^{\omega_k z} \tag{1.1}$$

with arbitrary complex exponents ω_k, absolutely convergent uniformly in $\mathfrak{B}$. This class of functions will be denoted as $\mathfrak{P}(\Omega, \mathfrak{B})$, where Ω denotes the set of exponents ω_k. Since a linear transformation in z has a trivial effect on the results we may assume that $\mathfrak{B}$ contains the points $z = 0$ and $z = 1$. Obviously, the class $\mathfrak{P}(\Omega, \mathfrak{B})$ is not affected if $\mathfrak{B}$ is replaced by its closed convex hull, and we may assume from the start that $\mathfrak{B}$ is closed and convex. Then $\mathfrak{B}$ either contains interior points and the elements of $\mathfrak{P}(\Omega, \mathfrak{B})$ are functions analytic in the region $\mathfrak{B}$, or $\mathfrak{B}$ is an interval of the real axis and the elements of $\mathfrak{P}(\Omega, \mathfrak{B})$ are continuous. In either case all the functions in $\mathfrak{P}(\Omega, \mathfrak{B})$ are bounded.

Let Ω_0 denote the set of complex numbers that are linear combinations with nonnegative coefficients of the $\omega_k \in \Omega$. The class $\mathfrak{P}(\Omega_0, \mathfrak{B})$ is a commutative algebra over the complex numbers if addition and multiplication of elements in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ and multiplication by complex numbers are defined in the obvious way. The algebra has a unit, which is the function identically 1 in $\mathfrak{B}$. The algebra is normed if we define the norm of the element $f(z) = \Sigma\, a_k \exp(\omega_k z)$ to be

$$\| f \| = \sup_{z \in \mathfrak{B}} \sum_k | a_k e^{\omega_k z} |. \tag{1.2}$$

Although we shall make no use of it we mention the fact that the underlying normed vector space is complete, hence $\mathfrak{P}(\Omega_0, \mathfrak{B})$ is a Banach space. As an immediate consequence we see that if $f \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ and $\| f - 1 \| < 1$ then $\frac{1}{f} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$; indeed $\frac{1}{f} = \sum_{k=0}^{\infty} (1 - f)^k$.

If $w = (w^{(1)}, \ldots, w^{(n)})$ is a vector and $A = (A^{(11)}, \ldots, A^{(nn)})$ is a matrix then $w \in \mathfrak{P}(\Omega_0, \mathfrak{B})$, $A \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ are to mean that $w^{(i)} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$, $A^{(ij)} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ for $i, j = 1, \ldots, n$. We also put $\| w \| = \sum_i \| w^{(i)} \|$, $\| A \| = \Sigma_{i,j} \| A^{(ij)} \|$, so that $\| Aw \| \leqq \| A \| \cdot \| w \|$ and also $\| AB \| \leqq \| A \| \cdot \| B \|$ if the vector w and the matrices A, B are in $\mathfrak{P}(\Omega_0, \mathfrak{B})$.

It is not necessary that the expansions (1.1) be absolutely and uniformly convergent in $\mathfrak{B}$ and that the norm (1.2) be chosen. Instead, we may interpret $\mathfrak{P}(\Omega_0, \mathfrak{B})$ as any normed algebra of complex-valued functions f over $\mathfrak{B}$ possessing absolutely convergent expansions $f(z) = \sum_k a_k \exp(\omega_k z)$ $(\omega_k \in \Omega_0)$. Although in the following we shall always speak of absolute and uniform convergence in $\mathfrak{B}$, the more general interpretation of convergence may be substituted without change.

2. The Expansion Theorem.

The differential systems to be considered here are of the form

$$\frac{dw}{dz} = A_0 w + \lambda A(z)\, w, \tag{2.1}$$

where A_0 is constant matrix, $A \in \mathfrak{P}(\Omega, \mathfrak{B})$, and λ a complex parameter. If $\mathfrak{B}$ has interior points we seek a solution w analytic in $\mathfrak{B}$; if $\mathfrak{B}$ is a real interval w is to be a differentiable

function of the real variable z. A fundamental solution of (2. 1) is a set of n solutions $w_i = (w_i^{(1)}, \ldots, w_i^{(n)})$ such that the matrix $W = (w_i^{(1)}, \ldots, w_i^{(n)})$ is nonsingular for $z \in \mathfrak{B}$. W satisfies the matrix equation

$$\frac{dW}{dz} = A_0 W + \lambda A(z)\, W \tag{2. 2}$$

and if W' is another fundamental solution of (2. 1) then $W' = WC$, where C is a nonsingular constant matrix.

Let $\sigma_1, \ldots, \sigma_m (m \leqq n)$ be the distinct characteristic values of the matrix A_0. We prove the following main result of this paper.

Theorem 2. 1. *If there exists a positive δ such that*

$$|\, \omega + \sigma_i - \sigma_j \,| \geqq \delta \text{ for } \omega \in \Omega_0,\ \omega \neq 0;\ i, j = 1, \ldots, m \tag{2. 3}$$

then system (2. 1) *has, for all sufficiently small λ, a fundamental solution W of the form*

$$W(z) = U(z)\, e^{Tz}, \tag{2. 4}$$

where U, $\frac{dU}{dz}$ and U^{-1} are in $\mathfrak{P}(\Omega_0, \mathfrak{B})$, $\lim\limits_{\lambda \to 0} \| U(z) - 1 \| = 0$, and T is a constant matrix, $\lim\limits_{\lambda \to 0} \| T - A_0 \| = 0$.

Proof. We construct an expansion of U. For this purpose let the sequences of nonnegative integers only a finite number of which are $\neq 0$ be arranged as a sequene $N_0, N_1, N_2, \ldots$ in such way that $N_r + N_s = N_t$ implies $r + s \leqq t$ (for details see [4]). Here $N_r + N_s$ denotes the usual sum of the sequences N_r, N_s, and N_0 denotes $(0, 0, \ldots)$. Also let

$$\begin{aligned} N_{(1)} &= (1, 0, 0, \ldots) \\ N_{(2)} &= (0, 1, 0, \ldots) \\ &\ldots\ldots \end{aligned} \tag{2. 5}$$

and put

$$N_r \cdot \Omega = \sum_{k \geqq 1} n_k \omega_k,\ |\, N_r \,| = \sum_{k \geqq 1} n_k \tag{2. 6}$$

if $N_r = (n_1, n_2, \ldots)$. $\mathfrak{N}$ is to denote the set of indices r such that $N_r \cdot \Omega = 0$. By assumption,

$$A(z) = \sum_{r \geqq 1} A_r\, e^{\omega_r z} = \sum_{r \geqq 1} A_r e^{N_{(r)} \cdot \Omega z}, \tag{2. 7}$$

where $A_1, A_2, \ldots$ are constant matrices and the sum (2. 7) is absolutely convergent uniformly in $\mathfrak{B}$. We set up

$$W(z) = (1 + \sum_{s \notin \mathfrak{N}} U_s e^{N_s \cdot \Omega z})\, e^{Tz} \tag{2. 8}$$

and seek to determine the constant matrices $T, U_1, U_2, \ldots$ so that (2. 8) satisfies (2. 2) formally. For this purpose we assume, for the moment, T as known and determine the U_t, $t \notin \mathfrak{N}$, from equations obtained by substituting (2. 7) and (2. 8) in (2. 2), expanding products according to $\exp\,(N_r \cdot \Omega z) \cdot \exp\,(N_s \cdot \Omega z) = \exp\,((N_r + N_s) \cdot \Omega z)$, and comparing coefficients. These equations are

$$U_t(N_t \cdot \Omega + T) - A_0 U_t = \lambda \sum_{(r,s)} A_r U_s,\ N_{(r)} + N_s = N_t \tag{2. 9}$$

where the sum is extended over all those r, s for which $N_{(r)} + N_s = N_t$, and where we have put $U_0 = 1$.

Equations (2. 9) form a recursive system for $U_1, U_2, \ldots$. We show that these matrices are uniquely determined as functions of T, $U_t = U_t(T)$, for any T for which $\| T - A_0 \|$ is sufficiently small. For the purpose of this proof we may assume that A_0 is in canonical form since we may look upon (2. 9) as an equation for CU_t where the nonsingular C is so chosen that CA_0C^{-1} is in canonical form (the subsequent expansions are not dependent on this assumption). We also make the assumption — to be removed in a minute — that the canonical A_0 has no non-zero off-diagonal terms. (2. 9) may be rewritten as

$$U_t(N_t \cdot \Omega + T - A_0) + U_t A_0 - A_0 U_t = \lambda \sum_{(r,s)} A_r U_s. \tag{2. 10}$$

Each component of the matrix equation

$$\omega U + U A_0 - A_0 U = V; \ \omega \in \Omega_0, \ \omega \neq 0 \tag{2. 11}$$

is of the form

$$(\omega + \sigma - \sigma')\, u = v \tag{2. 12}$$

where u, v are corresponding components of U, V, and σ, σ' are two characteristic values of A_0. Because of hypothesis (2. 3) we have a unique solution of (2. 12), hence of (2. 11), and $| u | \leqq \delta^{-1} | v |$, $\| U \| \leqq \delta^{-1} \| V \|$. It follows that if

$$\| T - A_0 \| \leqq \frac{\delta}{2} \tag{2. 13}$$

then the equation

$$U_t(N_t \cdot \Omega + T - A_0) + U_t A_0 - A_0 U_t = V, \ t \notin \mathfrak{N} \tag{2. 14}$$

can be solved for U_t. We write this solution as

$$U_t = \Gamma_t V \tag{2. 15}$$

where $\Gamma_t = \Gamma_t(T)$ is an operator on the n^2-dimensional vector space of the matrices V (Γ_t is not necessarily an $n \times n$ matrix). It also follows from (2. 3) and (2. 13) that

$$\| U_t \| \leqq \frac{2}{\delta} \| V \|, \tag{2. 16}$$

so that $\frac{2}{\delta}$ is a bound for $| \Gamma_t |$, the norm of the operator Γ_t. If the canonical form of A_0 is not diagonal, then A_0 can be considered as the limit of matrices whose canonical forms are diagonal. Since the above result is independent of whether A_0 has or does not have simple elementary divisors the same result can be derived for the more general A_0 by the limiting process.

Thus, (2. 10) leads to

$$U_t = \lambda \Gamma_t \sum_{(r,s)} A_r U_s, \ | \Gamma_t | \leqq \frac{2}{\delta} \tag{2. 17}$$

if T satisfies condition (2. 13). We now prove that the sum

$$\sum_{s \notin \mathfrak{N}} U_s(T)\, e^{N_s \cdot \Omega z} \tag{2. 18}$$

converges absolutely and uniformly in $\mathfrak{B}$ for any matrix T for which (2. 13) is satisfied. If we put

$$\hat{a}(z) = \sum_{r \geqq 1} \| A_r \| e^{\omega_r z} \tag{2. 19}$$

then the series

$$\hat{w}(z) = \sum_{n \geq 0} \left(\frac{2}{\delta}\right)^n |\lambda|^n \hat{a}^n(z) \tag{2.20}$$

converges absolutely uniformly in $\mathfrak{B}$ provided

$$|\lambda| < \frac{\delta}{2} \|A\|. \tag{2.21}$$

The same is true of the series

$$\hat{w}(z) = \hat{u}_0 + \sum_{s \notin \mathfrak{N}} \hat{u}_s e^{N_s \cdot \Omega z} \tag{2.22}$$

obtained from (2. 20) by substitution of (2. 19), multiplication of exponentials according to $\exp(N_r \cdot \Omega z) \cdot \exp(N_s \cdot \Omega z) = \exp((N_r + N_s) \cdot \Omega z)$, and combination of terms, consolidating all those for which $(N_r + N_s) \cdot \Omega = 0$ into the one term $\hat{u}_0$. The function $\hat{w}$ satisfies the equation

$$\hat{w} = 1 + \frac{2}{\delta} |\lambda| \hat{a}(z) \hat{w} \tag{2.23}$$

and the coefficients $\hat{u}_s$ can be obtained in a recursive way by substituting (2. 19) and (2. 22) in (2. 23). One obtains for $t \notin \mathfrak{N}$

$$\hat{u}_t = \frac{2}{\delta} |\lambda| \sum_{(r,s)} \|A_r\| \hat{u}_s, \quad N_{(r)} + N_s = N_t \tag{2.24}$$

where the sum is extended over all the r, s for which $N_{(r)} + N_s = N_t$. Comparing (2. 24) with (2. 17) one concludes that

$$\|U_t\| \leq \frac{\|U_0\|}{\hat{u}_0} \hat{u}_t, \; t \notin \mathfrak{N}. \tag{2.25}$$

Thus, the series (2. 18) is dominated by that in (2. 22) and its absolute and uniform convergence is proved.

We now form the sum

$$\sum_{(r',s')} A_{r'} U_{s'}(T), \quad (N_{(r')} + N_{s'}) \cdot \Omega = 0 \tag{2.26}$$

extended over all those r', s' for which $(N_{(r')} + N_{s'}) \cdot \Omega = 0$, and conclude from the above arguments that this sum is convergent. From the construction it follows that (2. 8) is a fundamental solution of (2. 1) if T is a solution of the *determining equation*

$$T - A_0 - \lambda \sum_{(r',s')} A_{r'} U_{s'}(T) = 0 \tag{2.27}$$

satisfying condition (2. 13). This equation has, for $\lambda = 0$, the solution $T = A_0$ and a nonvanishing Jacobian. Thus is has, for all sufficiently small λ, a unique solution T satisfying (2. 13) and such that $\lim_{\lambda \to 0} \|T - A_0\| = 0$. Since the constructed U is in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ so is $A_0 U - UT + \lambda A U$. Because of equations (2. 10) and (2. 27) the last expression is the termwise differentiated expansion of U. Thus $\frac{dU}{dz} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ and $W = U \exp(Tz)$ is a fundamental solution of (2. 1). It remains to prove $U^{-1} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$.

We consider the adjoint of system (2. 1)

$$\frac{dw}{d\bar{z}} = -A_0^* w - \bar{\lambda} A^*(\bar{z}) w \tag{2.28}$$

for w as a function of the complex variable $\bar{z}$, the conjugate of z. Here A_0^*, $A^*(\bar{z})$ are the conjugate transposes of $A_0, A(z)$. Since $A^*(\bar{z}) \in \mathfrak{P}(\bar{\Omega}_0, \mathfrak{B})$ and the characteristic

values of $-A_0^*$ are $-\bar{\sigma}_1, \ldots, -\bar{\sigma}_m$ condition (2. 3) is identical with the analogous condition for (2. 28). Thus, system (2. 28) has, for sufficiently small λ, a fundamental solution of the form $U_1(\bar{z}) \exp(T_1 \bar{z})$ with $U_1 \in \mathfrak{P}(\overline{\Omega}_0, \mathfrak{B})$. From the determining equation (see (2. 17) and (2. 27)) it can be concluded that

$$T_1 = -T^*. \tag{2. 29}$$

From the general theory of linear differential systems it is known that

$$\left(U_1(\bar{z})\, e^{T_1 \bar{z}}\right)^* U(z)\, e^{Tz} \tag{2. 30}$$

is a constant nonsingular matrix. Since $U \exp(Tz)$ may be multiplied by any nonsingular constant matrix we may assume that (2. 30) is the identity matrix. Using (2. 29) we find

$$U_1^*(z)\, U(z) = 1, \tag{2. 31}$$

where $U_1^*(z) \in \mathfrak{P}(\Omega_0, \mathfrak{B})$. Thus, U has an inverse $U^{-1} = U_1^*$ in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ if λ is chosen so small that a convergent expansion is obtained both for system (2. 1) and its adjoint (2. 28). (The existence of $U^{-1} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ could also be concluded from the expression for the inverse of a matrix and the remark about reciprocals in Section 1. However this would require a different restriction on λ). This completes the proof of Theorem 2. 1.

We give an explicit form to the recursion (2. 17). For $t = (1), (2), \ldots$ it gives

$$U_{(s)} = \lambda \Gamma_s A_s, \quad s = 1, 2, \ldots. \tag{2. 32}$$

If $s \neq (1), (2), \ldots$ then (2. 17) is applied again to U_s, and this is repeated until no U_s is left. One obtains

$$U_{s_1} = \lambda^f \Gamma_{s_1} \sum_{(r,s)} A_{r_1} \Gamma_{s_2} A_{r_2} \cdots \Gamma_{s_f} A_{r_f} \tag{2. 33}$$

where

$$\begin{aligned} N_{(r_1)} + N_{(r_2)} + \cdots + N_{(r_f)} &= N_{s_1}, \quad s_1 \notin \mathfrak{N} \\ N_{(r_2)} + \cdots + N_{(r_f)} &= N_{s_2}, \quad s_2 \notin \mathfrak{N} \\ \cdots \\ N_{(r_f)} &= N_{s_f}, \quad s_f \notin \mathfrak{N} \end{aligned} \tag{2. 34}$$

and the sum in (2. 33) is extended over all $r_1, \ldots, r_f, s_2, \ldots, s_f$ $(f \geqq 1)$ for which (2. 34) holds. From the first of the equations (2. 34) it is seen that

$$f = f(r_1) = |N_{r_1}|. \tag{2. 35}$$

If the fundamental solution W is replaced by $W' = WC$ where the constant matrix C is so chosen that $T' = C^{-1} TC$ is in canonical form then one obtains a fundamental solution

$$W' = U'(z)\, e^{T'z} \tag{2. 36}$$

of (2. 1), where $U' = UC \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ and T' is a constant matrix in canonical form. Thus it follows that there are complex numbers $\tau_1, \tau_2, \ldots, \tau_l$, nonnegative integers $n_1, n_2, \ldots, n_l$ with $n_1 + n_2 + \cdots + n_l = n$, and linearly independent vectors $u_1(z), \ldots, u_n(z)$ in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ such that

$$\begin{aligned} & u_1(z)\, e^{\tau_1 z}, [z u_1(z) + u_2(z)]\, e^{\tau_1 z}, \ldots, \left[\frac{z^{n_1-1}}{(n_1-1)!}\, u_1(z) + \cdots + u_{n_1}(z)\right] e^{\tau_1 z}, \\ & \ldots \\ & u_{n-n_l+1}(z)\, e^{\tau_l z}, [z u_{n-n_l+1}(z) + u_{n-n_l+2}(z)]\, e^{\tau_l z}, \ldots, \\ & \qquad \left[\frac{z^{n_l-1}}{(n_l-1)!}\, u_{n-n_l+1}(z) + \cdots + u_n(z)\right] e^{\tau_l z} \end{aligned} \tag{2. 37}$$

form a fundamental system of solutions of (2. 1). The numbers $\tau_1, \ldots, \tau_l$ (not necessarily distinct) are the *characteristic exponents* of system (2. 1), the integers $n_1, \ldots, n_l$ are their multiplicities. As $\lambda \to 0$ each of the τ_i converges to one of the σ_i (the characteristic values of A_0).

3. Reducibility, Uniqueness.

The factor U of the fundamental solution $W = U \exp(Tz)$ for system (2. 1) satisfies the differential equation

$$\frac{dU}{dz} + UT = A_0 U + \lambda A(z)\, U. \tag{3. 1}$$

If we make the substitution

$$w = Uv \tag{3. 2}$$

in (2. 1), replacing w by v, then using (3. 1) system (2. 1) becomes

$$\frac{dv}{dz} = Tv. \tag{3. 3}$$

Thus, (2. 1) is reduced to a system with constant coefficients. We say, system (2. 1) is "*reducible* $\mathfrak{P}(\Omega_0, \mathfrak{B})$". This is to indicate that, in the substitution $w = Uv$, U, $\frac{dv}{dz}$ and U^{-1} are in $\mathfrak{P}(\Omega_0, \mathfrak{B})$. (For the general concept of reducibility see Liapounoff [7], Erugin [2]). The content of Theorem 2. 1 can now be stated as follows:

If $|N_r \cdot \Omega + \sigma_i - \sigma_j| \geqq \delta > 0$ *for* $r \notin \mathfrak{N}$ *and* $i, j = 1, \ldots, m$ *then system* (2. 1) *is reducible* $\mathfrak{P}(\Omega_0, \mathfrak{B})$ *for all sufficiently small* λ.

The reduction process may be carried out in steps. Assume $A_0, A_1 \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ and consider the system

$$\frac{dw}{dz} = A_0(z)\, w + \lambda A_1(z)\, w. \tag{3. 4}$$

Suppose this system is reducible $\mathfrak{P}(\Omega_0, \mathfrak{B})$ for $\lambda = 0$; that is, there exists a fundamental solution $W_0 = U_0 \exp(T_0 z)$ of the system $\frac{dw}{dz} = A_0 w$, with U_0 and U_0^{-1} in $\mathfrak{P}(\Omega_0, \mathfrak{B})$. Then put $w = U_0 v$ and (3. 4) becomes

$$\frac{dv}{dz} = T_0 v + \lambda\, U_0^{-1} A_1 U_0 v. \tag{3. 5}$$

Since $U_0^{-1} A_1 U_0 \notin \mathfrak{P}(\Omega_0, \mathfrak{B})$ there is, for sufficiently small λ, a fundamental solution of (3. 5) of the form $V = U_1 \exp(T_1 z)$ with U_1 and U_1^{-1} in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ provided $|N_r \cdot \Omega + \sigma_i - \sigma_j| \geqq \delta > 0$ for $r \notin \mathfrak{N}$, σ_i being the characteristic values of T_0. The resulting $W = U_0 U_1 \exp(T_1 z)$ is a fundamental solution of (3. 4), with $U_0 U_1$ and $(U_0 U_1)^{-1}$ in $\mathfrak{P}(\Omega_0, \mathfrak{B})$.

The question arises as to the uniqueness of the characteristic exponents $\tau_1, \ldots, \tau_l$ and their multiplicities $n_1, \ldots, n_l$ in the representation $W = U \exp(Tz)$ of a fundamental solution. Here it is assumed that U and U^{-1} are in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ and that T is in canonical form. Of course only relative uniqueness, "uniqueness modulo Ω_0" can be meant here. Indeed if $\omega_1, \ldots, \omega_l$ are any numbers in Ω_0 such that $-\omega_1, \ldots, -\omega_l$ are also in Ω_0, then let $E(z)$ be the diagonal matrix whose first n_1 diagonal elements are $\exp(\omega_1 z)$, next n_2 diagonal elements are $\exp(\omega_2 z)$, etc. Then $E^{-1}(z) \exp(Tz) = \exp(T'z)$, where T'

is like T with τ_i replaced by $\tau_i - \omega_i$ $(i = 1, \ldots, l)$. Thus $W' = U' \exp(T'z)$ is also a fundamental solution and $U' = UE$, $U'^{-1} = E^{-1}U^{-1}$ in $\mathfrak{P}(\Omega_0, \mathfrak{B})$; the new characteristic exponents τ_i differ from the τ_i by $\omega_i \in \Omega_0$. We show that this is the only ambiguity in the characteristic exponents in the case where the functions in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ have *unique expansions*. This is to mean: If the ω_k are distinct numbers of Ω_0, if $\sum_k a_k \exp(\omega_k z) = 0$ the sum being absolutely and uniformly convergent in $\mathfrak{B}$, then $a_1 = a_2 = \cdots = 0$. We prove

Theorem 3. 1. *If the functions in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ have unique expansions then the characteristic exponents of system* (2. 1) *and their multiplicities are unique modulo Ω_0.*

Proof. Assume $U \exp(Tz)$ and $U' \exp(T'z)$ are both solutions of (2. 1) with U, U^{-1}, U', U'^{-1} in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ and T, T' in canonical form. Then there exists a nonsingular constant matrix C such that

$$U'(z)\, e^{T'z} = U(z)\, e^{Tz}\, C, \tag{3. 6}$$

hence

$$U^{-1}(z)\, U'(z)\, C^{-1} = e^{-T'z} e^{Tz}. \tag{3. 7}$$

Therefore $E = \exp(-T'z) \exp(Tz) \in \mathfrak{P}(\Omega_0, \mathfrak{B})$, and since the derivatives of U, U' are in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ we also have $\frac{dE}{dz} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$. Suppose τ_i, τ_i' are the characteristic numbers in the j-th diagonal position of T, T' respectively. We have

$$E^{(jj)} = \exp(\tau_i - \tau_i')\, z \in \mathfrak{P}(\Omega_0, \mathfrak{B})$$

and because of the uniqueness of expansions $\tau_i - \tau_i' \in \Omega_0$. In the same way it follows that $\tau_i' - \tau_i \in \Omega_0$. Let n_1, n_1' be the multiplicities of τ_1, τ_1' respectively, and assume $n_1 < n_1'$. Then there is a number $n < n_1'$ such that the n-th column of $\exp(Tz)$ contains only one nonzero element, $\exp(\tau_1 z)$, in its n-th row. Since the element in the $(n+1)$-th row and n-th column of $\exp(-T'z)$ is $-z \exp(-\tau_i' z)$ we obtain

$$E^{(n+1,n)} = -z \exp(\tau_1 - \tau_1') \in \mathfrak{P}(\Omega_0, \mathfrak{B}).$$

Thus, $z \in \mathfrak{P}(\Omega_0, \mathfrak{B})$, say $z = \sum_k a_k \exp(\omega_k z)$, where the ω_k are distinct numbers in Ω_0. Since we can differentiate termwise we also have $1 = \Sigma a_k \omega_k \exp(\omega_k z)$, which contradicts the uniqueness of expansions in $\mathfrak{P}(\Omega_0, \mathfrak{B})$. Thus $n_1 \geqq n_1'$, and since the opposite inequality follows in the same way, we have proved $n_1 = n_1'$. The same argument is valid for the multiplicities $n_2, \ldots, n_l$ and the proof of Theorem 3. 1 is complete.

4. Particular Exponent Sets.

We observe that if both $\tau_1, \ldots, \tau_l$ and $\tau_1', \ldots, \tau_l'$ are characteristic exponents of system (2. 1) then, by Theorem 3. 1 $\tau_i - \tau_i' \in \Omega_0$ and $\tau_i' - \tau_i \in \Omega_0 (i = 1, \ldots, l)$. This is due to our assumption that in the representation $W = U \exp(Tz)$ of a fundamental solution both U and U^{-1} are in $\mathfrak{P}(\Omega_0, \mathfrak{B})$. A consequence of this is that if $N_r \cdot \Omega \neq 0$ for $r \geqq 1$ then the characteristic numbers are unique in the absolute sense.

The hypothesis $N_r \cdot \Omega \neq 0$ for $r \geqq 1$ has other important implications. Since in this case $\mathfrak{N}$ consists of 0 only, the determining equation (2. 27) becomes simply $T - A_0 = 0$. Thus the characteristic exponents coincide with the characteristic values of A_0, no matter what λ is. If, moreover, $|N_r \cdot \Omega| \to \infty$ as $r \to \infty$ then the expansions of Section 2 converge for all λ, so that there is no need for a parameter in system (2. 1). More precisely, we have

Theorem 4. 1. *If the set Ω_0 has no finite limit point and*

$$N_r \cdot \Omega + \sigma_i - \sigma_j \neq 0, \; r \geqq 1; \; i, j = 1, \ldots, m, \tag{4. 1}$$

then the system

$$\frac{dw}{dz} = A_0 w + A(z)\, w \tag{4. 2}$$

with $A \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ has a fundamental solution of the form $W = U \exp(A_0 z)$ with U and U^{-1} in $\mathfrak{P}(\Omega_0, \mathfrak{B})$. If moreover the functions in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ have unique expansions and $W = U \exp(Tz)$ is any solution of (4. 2) with U and U^{-1} in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ then T is similar to A_0.

Proof. Since $T = A_0$ is a solution of the determining equation and since for $T = A_0$ equation (2. 10) with $\lambda = 1$ has because of (4. 1) a unique solution $U_t = \Gamma_t \sum_{(r,s)} A_r U_s$, all that remains to be proved is that the expansion (2. 8) converges for $\lambda = 1$ absolutely and uniformly in $\mathfrak{B}$. By hypothesis we have $|N_r \cdot \Omega| \to \infty$ as $r \to \infty$; hence, we can choose r_0 so large that

$$|N_r \cdot \Omega + \sigma_i - \sigma_j| \geqq 2 \, \| A \|, \; r \geqq r_0; \; i, j = 1, \ldots, m. \tag{4. 3}$$

Then, following the proof of Theorem 2. 1, it is seen that $|\Gamma_t| \leqq \frac{1}{2} \| A \|$ for $t \geqq r_0$ and that expansion (2. 8) converges. This completes the proof of Theorem 4. 1.

We observe that the hypothesis $|N_r \cdot \Omega| \to \infty$ as $r \to \infty$ is implied by the assumption that the set Ω has no finite limit point and lies in an open half-plane. Under this assumption the equation $\omega_r + \omega_s = \omega_t$ $(\omega_r, \omega_s, \omega_t \in \Omega_0)$, ω_t fixed, has but a finite number of solutions ω_r, ω_s, and the straightforward method of substituting the expansion $U(z) = \Sigma U_t \exp(\omega_t z)$ — where the sum is extended over all the distinct $\omega_t \in \Omega_0$ — in the equation

$$\frac{dU}{dz} = A(z)\, U + A_0 U - U A_0 \tag{4. 4}$$

and of comparing coefficients leads to a sequence of finite algebraic systems for the coefficients U_t. This result or other essentially equivalent to it seem to have been known.

If the set Ω does not lie in a closed half-plane then Ω_0 is either dense in the complex plane or Ω_0 is discrete. The first case violates condition (2. 3) no matter what the characteristic values σ_i of A_0 are; it is excluded here. In the second case Ω_0 is the lattice of points $\{\nu_1 \omega_1^0 + \nu_2 \omega_2^0\}$ where ω_1^0, ω_2^0 are two complex numbers with nonreal ratio $\frac{\omega_1^0}{\omega_2^0}$ and ν_1, ν_2 run through all the integers. For this case we prove

Theorem 4. 2. *If the set Ω_0 is the lattice $\{\nu_1 \omega_1^0 + \nu_2 \omega_2^0; \; \nu_1, \nu_2 = 0, \pm 1 \pm 2, \ldots\}$ then system (2. 1) with $A \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ has, for all sufficiently small λ, a fundamental solution of the form $W = U \exp(Tz)$ with U and U^{-1} in $\mathfrak{P}(\Omega_0, \mathfrak{B})$.*

Proof. Let R be a diagonal matrix whose characteristic values are in Ω_0 and which commutes with A_0. The substitution $w = \exp(Rz)\, v$ transforms system (2. 1) into

$$\frac{dv}{dz} = (A_0 - R)\, v + \lambda e^{-Rz} A(z)\, e^{Rz} v. \tag{4. 5}$$

Since $\exp(-Rz)\, A(z) \exp(Rz) \in \mathfrak{P}(\Omega_0, \mathfrak{B})$, Theorem 2. 1 applies to (4. 5). If $V = U' \exp(Tz)$ is a fundamental solution of (4. 5) with $U', U'^{-1} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ then $W = U \exp(Tz)$ with $U = \exp(Rz)\, U'$, $U^{-1} = U'^{-1} \exp(-Rz)$ in $\mathfrak{P}(\Omega_0, \mathfrak{B})$ is a fundamental solution of (2. 1). We show that R can be so chosen that condition (2. 3) is satisfied for system (4. 5).

Let the disjoint index sets I, J be so chosen that

$$(4.6)\qquad \begin{aligned} &\sigma_i - \sigma_j = \omega_i \text{ for } i \in I,\ j \in J \\ &\sigma_i - \sigma_j \not\equiv 0 \pmod{\Omega_0} \text{ for } (i, j) \notin I \times J \end{aligned}$$

where $\omega_i \in \Omega_0$. Let R be the diagonal matrix with component ω_i where A_0 has $\sigma_i (i \in I)$, all the other components being 0. Then if $\varrho_1, \ldots, \varrho_m$ denote the characteristic values of $A_0 - R$ it is easily verified that $\varrho_i - \varrho_j = 0$ if $i \in I$, $j \in J$ and $\varrho_i - \varrho_j \not\equiv 0 \pmod{\Omega_0}$ otherwise. Thus

$$(4.7)\qquad \omega + \varrho_i - \varrho_j \neq 0 \text{ for } \omega \in \Omega_0,\ \omega \neq 0;\ i, j = 1, \ldots, m$$

and condition (2. 3) is satisfied for system (4. 5). This completes the proof of Theorem 4. 2.

The restriction to small values of λ in Theorem 4. 2 can also, to a certain extent, be done away with. Let $\lambda_1, \lambda_2, \ldots$ be a sequence of values of the parameter λ for which Theorem 4. 2 holds, and let $\lambda_0 = \lim \lambda_\nu$ be a value for which Theorem 4. 2 does not hold. Let $W_\nu = U_\nu \exp(T_\nu z)$ $(\nu = 1, 2, \ldots)$ be fundamental solutions corresponding to λ_ν, chosen so that T_ν is in canonical form. By modifying U_ν, if necessary, one can arrive at T_ν all of whose characteristic values lie in the parallelogram with vertices 0, ω_1^0, ω_2^0, $\omega_1^0 + \omega_2^0$. Thus a subsequence of the T_ν converges, we may assume

$$(4.8)\qquad \lim_{\nu \to \infty} T_\nu = T_0.$$

By multiplying, if necessary, $U_\nu \exp(T_\nu z)$ by a constant factor one can attain $\| U_\nu \| = 1 (\nu = 1, 2, \ldots)$. Then a subsequence of $W_\nu(z) = U_\nu(z) \exp(T_\nu z)$ may be chosen — let it be denoted by $W_1, W_2, \ldots$ again — such that the sequence $W_1(0), W_2(0), \ldots$ converges. It then follows from the general theory of linear differential equations that

$$(4.9)\qquad \lim_{\nu \to \infty} W_\nu(z) = W_0(z)$$

uniformly for $z \in \mathfrak{B}$ and that W_0 is a fundamental solution of (2. 1) for $\lambda = \lambda_0$. Equations (4. 8) and (4. 9) imply

$$(4.10)\qquad \lim_{\nu \to \infty} U_\nu(z) = U_0(z)$$

uniformly for $z \in \mathfrak{B}$. Since W_0 is nonsingular the same is true of U_0, and by (4. 10)

$$(4.11)\qquad \lim_{\nu \to \infty} U_\nu^{-1}(z) = U_0^{-1}(z)$$

uniformly for $z \in \mathfrak{B}$. In general, (4. 10), (4. 11) do not imply that U_0, U_0^{-1} are in $\mathfrak{P}(\Omega_0, \mathfrak{B})$. However if they are, or if U_0, $U_0^{-1} \in \mathfrak{P}(\Omega_0, \mathfrak{B}')$, where $\mathfrak{B}' < \mathfrak{B}$, then substitution of $w = U_0 v$ in (2. 1) gives

$$(4.12)\qquad \frac{dv}{dz} = T_0 v + (\lambda - \lambda_0)\, U_0^{-1}(z)\, A(z)\, U_0(z)\, v$$

and this system has, by Theorem 4. 2, for $|\lambda - \lambda_0|$ sufficiently small, a fundamental solution of the form $V = U_1 \exp(T_1 z)$ with U_1, $U_1^{-1} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$. Then $W = U_0 U_1 \exp(T_1 z)$ is a fundamental solution of (2. 1) with $U_0 U_1$ and $(U_0 U_1)^{-1}$ in $\mathfrak{P}(\Omega_0, \mathfrak{B})$, valid for λ values beyond those for which Theorem 4. 2holds.

Another noteworthy special case of system (2. 1) is where the matrix A_0 commutes with the matrices A_r, $r \geqq 1$. Then if we can show that the solution T of the determining equation commutes with A_0 we find from (2. 10) that both $A_0 U_t$ and $U_t A_0 (t \in \mathfrak{N})$ satisfy the same recursion, hence $A_0 U_t = U_t A_0$ and $A_0 U = U A_0$. The operator for Γ_t becomes

in this case post-multiplication by the matrix $(N_t \cdot \Omega + T - A_0)^{-1}$ and condition (2. 3) may be replaced by $|\omega| \geqq \delta$ $(\omega \in \Omega_0,\ \omega \neq 0)$. When the expansion (2. 33) for $U_s(T)$ is substituted in (2. 27) it is seen that the determining equation is a power series in T with coefficients that are power series in $A_0, A_1, A_2, \ldots$. Therefore, the solution T can be written as a power series in $A_0, A_1, A_2, \ldots$ and it follows that $TA_0 = A_0 T$. We have proved

Theorem 4. 3. *If* 0 *is an isolated point of* Ω_0 *and* $A_0 A_r = A_r A_0 (r \geqq 1)$ *then system* (2. 1) *with* $A \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ *has, for all sufficiently small* λ, *a fundamental solution* $W = U \exp(Tz)$ *where* $U, U^{-1} \in \mathfrak{P}(\Omega_0, \mathfrak{B})$ *and* $A_0 T = TA_0$, $A_0 U = UA_0$.

5. Special Cases.

We exhibit a few simple special cases where the hypotheses of the above theorems are satisfied. The ensuing conclusions are, in several cases, known.

1. $\mathfrak{B}$ is the real axis; Ω consists of $i\omega$, $-i\omega (\omega > 0)$. Then $\mathfrak{P}(\Omega_0, \mathfrak{B})$ is the class of periodic functions of the real variable $z = x$ possessing period $\frac{2\pi}{\omega}$ and absolutely and uniformly convergent Fourier expansions. System (2. 1) is of the form

$$\frac{dw}{dx} = A_0 w + \lambda \sum_{r=-\infty}^{\infty} A_r e^{ir\omega x} w. \tag{5. 1}$$

There is no restiction on the characteristic values σ_i of the matrix A_0 if the substitution $w = \exp(Rx)\, v$ mentioned in the proof for Theorem 4. 2 is made use of. Also, the restriction to small values of λ is unessential as the remarks following Theorem 4. 2 show.

2. $\mathfrak{B}$ is the real axis; Ω consists of the numbers $i\omega_1, i\omega_2, \ldots$ where $\omega_1, \omega_2, \ldots$ are real numbers bounded from one side and having no finite limit point. Then $\mathfrak{P}(\Omega_0, \mathfrak{B})$ is a class of almost periodic functions of the real variable $z = x$ having absolute and uniformly convergent nonharmonic Fourier expansions. Here Theorem 4. 1 applies so that there is no restriction on λ. The system is of the form

$$\frac{dw}{dx} = A_0 w + A(x)\, w, \tag{5. 2}$$

the components of $A(x)$ being almost periodic functions of the above class. Each solution is a linear combination of functions of the form $x^k \exp(\tau x)\, u(x)$, where $u(x)$ is an almost periodic function of the above class and τ is a characteristic value of A_0 (for related results see Putnam and Wintner [11]).

3. $\mathfrak{B}$ is the half-line $-\infty < \operatorname{Re} z \leqq 0$, $\operatorname{Im} z = 0$; Ω consists of the positive numbers $\varrho_1, \varrho_2, \ldots$ which have no finite limit points. With the transformation $\exp z = x$, $\mathfrak{P}(\Omega_0, \mathfrak{B})$ becomes the class of continuous functions of the real variable x defined on $0 \leqq x \leqq 1$ and having an absolutely and uniformly convergent expansion in nonnegative integral powers of $x^{\varrho_1}, x^{\varrho_2}, \ldots$. Theorem 4. 1 applies again. The transformed system is of the form

$$x \frac{dw}{dx} = A_0 w + \left(\sum_{r \geqq 1} A_r x^{N_r \cdot P} \right) w \tag{5. 3}$$

where P denotes the sequence $\varrho_1, \varrho_2, \ldots$. Each solution is a linear combination of functions having expansions of the form $x^\tau (\log x)^k \sum a_r x^{N_r \cdot P}$, where τ is a characteristic value of A_0.

4. $\mathfrak{B}$ is the rectangle $\log a \leqq \operatorname{Re} z \leqq \log b$, $0 \leqq \operatorname{Im} z \leqq 2\pi$; Ω consists of the numbers $1, -1$. With the transformation $\exp z = \zeta$, $\mathfrak{P}(\Omega_0, \mathfrak{B})$ becomes the class of functions analytic and single-valued in the ring $a \leqq |\zeta| \leqq b$ and having Laurent expansions $\sum_{r=-\infty}^{+\infty} a_r \zeta^r$ converging absolutely and uniformly in this ring. The transformed system (2. 1) is of the form

$$\zeta \frac{dw}{d\zeta} = A_0 + \lambda \left(\sum_{r=-\infty}^{+\infty} A_r \zeta^r \right) w \tag{5. 4}$$

and condition (2. 3) is $\sigma_i - \sigma_j \neq k$ $(i, j = 1, \ldots m;\ k = 1, 2, \ldots)$. As shown in the proof of Theorem 4. 2, this condition is not essential and can be disposed of by a simple substitution for w. Also the restriction to small values of λ can be circumvented by the continuation process described in Section 4. Each solution is a linear combination of functions having expansions of the form $\zeta^\tau (\log \zeta)^k \sum_{r=-\infty}^{+\infty} a_r \zeta^r$. Whereas the formal expansions of the classical theory in the neighborhood of irregular singularities are in general divergent (asymptotically convergent), the expansions obtained here are convergent.

To illustrate this important point we give two examples.

Example 5. 1. Consider the differential equation

$$\zeta \frac{dw}{d\zeta} = 2(\zeta^2 + \zeta^{-2})\, w \tag{5. 5}$$

near the singularity of the second kind $\zeta = 0$. We seek a solution having the expansion

$$w = 1 + \sum_{r \in \mathfrak{N}} u_r \zeta^{N_r \cdot \Omega}, \tag{5. 6}$$

anticipating that the characteristic exponent is $\tau = 0$. We order the pairs N_r of nonnegative integers so that $N_r = (k, n-k)$ where $r = \frac{1}{2} n(n+1) + k$ $(k = 0, 1, \ldots, n;\ n = 1, 2, \ldots)$ and $N_r \cdot \Omega = -n + 2k$. The recursion formula (2. 17) becomes $u_0 = 1$, $u_1 = u_2 = 0$ and for $n = 2, 3, \ldots$

$$(-n + 2k)\, u_{\frac{1}{2}n(n+1)+k} = \begin{cases} 2u_{\frac{1}{2}(n-2)(n-1)+k} + 2u_{\frac{1}{2}(n-2)(n-1)+k-2}, \\ \qquad \text{for } k = 2, \ldots, n-2;\ k \neq \frac{1}{2}n, \\ 2u_{\frac{1}{2}(n-2)(n-1)+k}, \quad \text{for } k = 0, 1, \\ 2u_{\frac{1}{2}(n-2)(n-1)+k-2}, \text{ for } k = n-1,\ n. \end{cases} \tag{5. 7}$$

The index $k = \frac{1}{2}n$ is omitted so as to exclude the u_r with $r \in \mathfrak{N}$. It is readily seen that the $u's$ in (5. 7) with n odd or $-\frac{1}{2}n + k$ odd are 0. Using this fact, (5. 7) may be rewritten as

$$u_r = \begin{cases} \dfrac{1}{r - 2m(m+1)} (u_{r-4m+1} + u_{r-4m-1}), \\ \qquad \text{for } r = m(2m+1) + 2, \ldots, m(2m+1) + 2m - 2;\ r \neq 2m(m+1), \\ \dfrac{1}{r - 2m(m+1)} u_{r-4m+1}, \quad \text{for } r = m(2m+1), \\ \dfrac{1}{r - 2m(m+1)} u_{r-4m+1}, \quad \text{for } r = m(2m+1) + 2m, \end{cases} \tag{5. 8}$$

for $m = 1, 2, \ldots$; all the remaining u_r are 0.

One observes from (5. 8) that for $m = 1, 2, \ldots$

$$\begin{aligned} u_{4m(2m+1)+2k} &= u_{4m(2m+1)-2k}, & k &= 1, \ldots, m, \\ u_{4(m+1)(2m+1)+2k-1} &= -u_{4(m+1)(2m+1)-(2k-1)}, & k &= 1, \ldots, m+1. \end{aligned} \tag{5. 9}$$

From the second of these relations it follows in particular that the sum in the determining equation (2. 27) vanishes, which verifies the solution $\tau = 0$.

We have established the expansion

$$(5.10)\qquad \begin{aligned} w = 1 &+ \frac{1}{1!}(\zeta^2 - \zeta^{-2}) + \frac{1}{2!}(\zeta^4 + \zeta^{-4}) + \frac{1}{3!}(\zeta^6 + 3\zeta^2 + 3\zeta^{-2} + \zeta^{-6}) \\ &+ \frac{1}{4!}(\zeta^8 + 8\zeta^4 + 8\zeta^{-4} + \zeta^{-8}) + \cdots. \end{aligned}$$

It is an expansion of the solution $w = a^{-1}\exp(\zeta^2 - \zeta^{-2})$ of (5. 5), where

$$a = \sum_{k \geqq 0} \frac{(-1)^k}{(k!)^2}$$

is the constant term in the expansion $\sum_{k \geqq 0} \frac{1}{k!}(\zeta^2 - \zeta^{-2})^k$ of $\exp(\zeta^2 - \zeta^{-2})$.

Example 5. 2. In this example we consider a system where the solution of the determining equation depends on λ. We start with the quite general equation of second order

$$(5.11)\qquad \zeta^2 \frac{d^2 u}{d\zeta^2} + \zeta \frac{du}{d\zeta} = \sigma^2 u + 2\lambda\sigma \left(\sum_{r=-\infty}^{\infty} a_r \zeta^r\right) u, \quad a_0 = 0$$

which on substitution of $2w^{(1)} = \sigma u + \zeta \frac{du}{d\zeta}$, $2w^{(2)} = \sigma u - \zeta \frac{du}{d\zeta}$ becomes the system

$$(5.12)\qquad \begin{gathered} \zeta \frac{dw}{d\zeta} = A_0 w + \lambda \left(\sum_{r=-\infty}^{\infty} a_r \zeta^r\right) A_1 w, \\ a_0 = 0, \quad A_0 = \begin{pmatrix} \sigma & 0 \\ 0 & -\sigma \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}. \end{gathered}$$

We assume here $\sigma \neq 0, \pm 1, \pm 2, \ldots$, although this hypothesis corresponding to condition (2. 3) could be dispensed with by a modified procedure. We determine a fundamental solution W with convergent expansion about the irregular singular point $\zeta = 0$,

$$(5.13)\qquad W = (U_0 + \sum_{s \in \mathfrak{R}} U_s \zeta^{N_s \cdot \Omega})\, \zeta^T,$$

where we choose for

$$(5.14)\qquad U_0 = \begin{pmatrix} \sigma - \tau_1 & \sigma - \tau_2 \\ \sigma + \tau_1 & \sigma + \tau_2 \end{pmatrix}$$

so as to obtain T in diagonal form, with characteristic values τ_1, τ_2. This setup will be justified by the result. The exponents $N_s \cdot \Omega$ in (5. 13) are integers $\varkappa \neq 0$; the matrices A_r of (2. 7) are here all of the same form, $A_r = a_{\varkappa'} A_1$ if $\varkappa' = N_r \cdot \Omega$. The operator Γ_s by which the matrix (u_{ij}) is obtained from the matrix (v_{ij}) $(i, j = 1, 2)$ — see (2. 15) — is defined by the relations

$$(5.15)\qquad \begin{aligned} u_{11} &= \frac{1}{\varkappa + \tau_1 + \sigma} v_{11}, & u_{12} &= \frac{1}{\varkappa + \tau_2 + \sigma} v_{12} \\ u_{21} &= \frac{1}{\varkappa + \tau_1 + \sigma} v_{21}, & u_{22} &= \frac{1}{\varkappa + \tau_2 + \sigma} v_{22} \end{aligned}$$

where $\varkappa = N_s \cdot \Omega$. To illustrate the result of the expansion (2. 33) we calculate

$$(5.16)\qquad \begin{gathered} \Gamma_s(A_1 U_0) = 2\sigma \begin{pmatrix} \dfrac{1}{\varkappa + \tau_1 - \sigma} & \dfrac{1}{\varkappa + \tau_2 - \sigma} \\ -\dfrac{1}{\varkappa + \tau_1 - \sigma} & -\dfrac{1}{\varkappa + \tau_2 - \sigma} \end{pmatrix} \\ \Gamma_s(A_1 U_0) = 4\sigma^2 \begin{pmatrix} f_1(\varkappa) & f_2(\varkappa) \\ -f_1(\varkappa) & -f_2(\varkappa) \end{pmatrix}, \end{gathered}$$

where we have introduced the abbreviation

$$f_i(\varkappa) = \frac{1}{(\varkappa + \tau_i)^2 - \sigma^2}, \quad i = 1, 2. \tag{5.17}$$

In this way one obtains the expansion

$$W = \left\{ U_0 + \sum_{j \geqq 1} (2\lambda\sigma)^{j+1} \sum_{(\varkappa)} a_{\varkappa_1} a_{\varkappa_2} \cdots a_{\varkappa_{j+1}} \zeta^{\varkappa} \right. \tag{5.18}$$

$$\left. \cdot \begin{pmatrix} \dfrac{f_1(\varkappa + \varkappa_1) \cdots f_1(\varkappa + \varkappa_1 + \cdots + \varkappa_j)}{\varkappa + \tau_1 - \sigma} & \dfrac{f_2(\varkappa + \varkappa_1) \cdots f_2(\varkappa + \varkappa_1 + \cdots + \varkappa_j)}{\varkappa + \tau_2 - \sigma} \\ \dfrac{f_1(\varkappa + \varkappa_1) \cdots f_1(\varkappa + \varkappa_1 + \cdots + \varkappa_j)}{-(\varkappa + \tau_1 + \sigma)} & \dfrac{f_2(\varkappa + \varkappa_1) \cdots f_2(\varkappa + \varkappa_1 + \cdots + \varkappa_j)}{-(\varkappa + \tau_2 + \sigma)} \end{pmatrix} \right\} \begin{pmatrix} \zeta^{\tau_1} & 0 \\ 0 & \zeta^{\tau_2} \end{pmatrix}.$$

Each $\varkappa_i$ in the sum is a positive or negative integer and the sum $\sum_{(\varkappa)}$ is extended over all systems $(\varkappa, \varkappa_1, \ldots, \varkappa_{j+1})$ for which

$$\begin{aligned} &\varkappa + \varkappa_1 + \varkappa_2 + \cdots + \varkappa_i \neq 0, \ 1 \leqq i \leqq j, \\ &\varkappa + \varkappa_1 + \varkappa_2 + \cdots + \varkappa_{j+1} = 0. \end{aligned} \tag{5.19}$$

These conditions correspond to (2. 34). Since

$$U_0 T - A_0 U_0 = \begin{pmatrix} \tau_1^2 - \sigma^2 & \tau_2^2 - \sigma^2 \\ -(\tau_1^2 - \sigma^2) & -(\tau_2^2 - \sigma^2) \end{pmatrix} \tag{5.20}$$

the determining equation — see (2. 27) — becomes

$$\begin{pmatrix} \tau_1^2 - \sigma^2 & \tau_2^2 - \sigma^2 \\ -(\tau_1^2 - \sigma^2) & -(\tau_2^2 - \sigma^2) \end{pmatrix} = \sum_{j \geqq 1} (2\lambda\sigma)^{j+1} \sum_{(\varkappa)} a_{\varkappa_1} a_{\varkappa_2} \cdots a_{\varkappa_{j+1}} \tag{5.21}$$

$$\cdot \begin{pmatrix} f_1(\varkappa_1) \cdots f_1(\varkappa_1 + \varkappa_2 + \cdots + \varkappa_j) & f_2(\varkappa_1) \cdots f_2(\varkappa_1 + \varkappa_2 + \cdots + \varkappa_j) \\ -f_1(\varkappa_1) \cdots f_1(\varkappa_1 + \varkappa_2 + \cdots + \varkappa_j) & -f_2(\varkappa_1) \cdots f_2(\varkappa_1 + \varkappa_2 + \cdots + \varkappa_j) \end{pmatrix},$$

where each $\varkappa_i$ is a positive or negative integer and the sum $\sum_{(\varkappa)}$ is extended over all systems $(\varkappa_1, \ldots, \varkappa_{j+1})$ for which

$$\begin{aligned} &\varkappa_1 + \varkappa_2 + \cdots + \varkappa_i \neq 0, \ 1 \leqq i \leqq j, \\ &\varkappa_1 + \varkappa_2 + \cdots + \varkappa_{j+1} = 0. \end{aligned} \tag{5.22}$$

Equation (5. 21) shows that the assumption that T is diagonal with characteristic values τ_1, τ_2 is justified. The matrix equation (5. 21) may be replaced by the one scalar equation

$$\tau^2 - \sigma^2 - \sum_{j \geqq 1} (2\lambda\sigma)^{j+1} \sum a_{\varkappa_1} a_{\varkappa_2} \cdots a_{\varkappa_{j+1}} f(\varkappa_1) \cdots f(\varkappa_1 + \varkappa_2 + \cdots + \varkappa_j) = 0, \tag{5.23}$$

where $f(\varkappa) = \dfrac{1}{(\varkappa + \tau)^2 - \sigma^2}$. The two roots $\tau = \tau_1$, τ_2 of (5. 23) which converge to $+\sigma$, $-\sigma$ as $\lambda \to 0$ are the characteristic exponents of W. (5. 23) together with (5. 18) gives the complete solution of system (5. 12) and equation (5. 11) (for a similar solution of Mathieu's and Hill's equations see Golomb [5]).

References.

[1] *L. Cesari*, Sulla stabilità delle soluzioni dei sistemi di equazioni differenziali lineari a coefficienti periodici, Mem. Accad. Italia Cl. Sci. Fis. Mat. Nat. (6), **11** (1941), 633—695.

[2] *N. P. Erugin*, Reducible systems, Trudy Math. Inst. Steklov **13** (1946), 1—95.

[3] *G. Floquet*, Sur les équations linéaires à coefficients périodiques, Annal. Sci. École Norm. Sup. (2), **12** (1883), 47—89.

[4] *M. Golomb*, Solution of certain nonautonomous differential systems by series of exponential functions, Illinois Journ. Math. **3** (1959), 45—65.

[5] *M. Golomb*, Expansion and boundedness theorems for solutions of linear differential systems with periodic or almost periodic coefficients, Archive Rational Mech. Anal. **2** (1958), 284—308.

[6] *J. K. Hale*, On boundedness of the solution of linear differential systems with periodic coefficients, Riv. Mat. Univ. Parma **5** (1954), 137—167.

[7] *A. Liapounoff*, Problème général de la stabilité du mouvement, Ann. Fac. Sci. Univ. Toulouse, **9** (1907); Ann. of Math. Study no. **17**, Princeton 1947.

[8] *A. Lindstedt*, Differentialgleichungen der Störungstheorie, Mém. Sci. St. Petersbourgh **31** (1883).

[9] *E. Picard*, Traité d'Analyse, **3**, Paris 1896.

[10] *J. H. Poincaré*, Les méthodes nouvelles de la mécanique céleste, **1**, Paris 1892.

[11] *C. R. Putnam* and *A. Wintner*, Linear differential equations with almost periodic or Laplace transform coefficients, Amer. Journ. Math. **73** (1951), 729—806.

[12] *Y. Sibuya*, Sur un système des équations différentielles ordinaires linéaires à coefficients périodiques et contenant des paramètres, Journ. Fac. Sci. Univ. Tokyo I, **7** (1954), 229—241.

[13] *Y. Sibuya*, Non-linear ordinary differential equations with periodic coefficients, Funkcialaj Ekvacioj **1** (1958), 121—204.

[14] *W. Wasow*, Solution of certain nonlinear differential equations by series of exponential functions, Illinois J. Math., **2** (1958), 254—260.

Eingegangen 14. Dezember 1959.

Bemerkungen zu den allgemeinen Dedekindschen Summen.

Von *C. Meyer* in Hamburg.

Die speziellen Dedekindschen Summen treten erstmalig in der von R. Dedekind [1] aufgestellten Transformationsformel auf, die das Verhalten des Logarithmus der Funktion $\eta(\tau) = \sqrt[24]{\Delta(\tau)}$ gegenüber Modulsubstitutionen beschreibt. Entsprechend treten die allgemeinen Dedekindschen Summen erstmalig in derjenigen Transformationsformel auf, die das Verhalten des Logarithmus der f-ten Teilwerte der Kleinschen σ-Funktion gegenüber Modulsubstitutionen beschreibt, und zwar handelt es sich dabei genauer um Substitutionen aus der Hauptkongruenzgruppe f-ter Stufe. Die genannten Transformationsformeln und damit die Dedekindschen Summen spielen in den Klassenzahluntersuchungen des Verfassers [3] eine wichtige Rolle, indem sie zur Bildung von elementar-arithmetischen Klasseninvarianten reell-quadratischer Zahlkörper Anlaß geben, eine Tatsache, die für quadratische Formen ebenfalls von H. Rademacher [5] bemerkt worden ist. Durch Charaktere linear kombiniert liefern diese Invarianten dann Ausdrücke, deren Produkt für die total-imaginären Klassenkörper zu reell-quadratischem Grundkörper das Analogon des ersten Klassenzahlfaktors von Kummer im Fall der absolut-abelschen Zahlkörper darstellt. Hierin wurzelt die Bedeutung der Dedekindschen Summen für die algebraische Zahlentheorie.

In Band 198 dieses Journals sind nun die Dedekindschen Summen, losgelöst von ihrer funktionentheoretischen Herkunft, vom Verfasser [4] besonders in Hinblick auf die Anwendungen des näheren untersucht worden. An die Arbeiten [3], [4] des Verfassers anknüpfend hat sodann kürzlich U. Dieter in Band 201 dieses Journals ganz allgemein das Transformationsverhalten des Logarithmus der Kleinschen σ-Teilwerte gegenüber beliebigen Modulsubstitutionen festgestellt und dabei das Reziprozitätsgesetz für die allgemeinen Dedekindschen Summen entdeckt, welches das wohlbekannte Gesetz von Dedekind verallgemeinert. Dieses allgemeinere Gesetz erweist sich wieder bei den Anwendungen in Funktionentheorie und Arithmetik als das zentrale Theorem der ganzen Theorie.

Im folgenden wird nunmehr eine Neubegründung der Dieterschen Ergebnisse gegeben, soweit sie das Reziprozitätsgesetz betreffen. Es gelingt nämlich, die von H. Rademacher [6] stammende Cotangentenformel für die speziellen Dedekindschen Summen zu verallgemeinern. Hierauf gestützt wird es dann möglich, die allgemeinen Dedekindschen Summen auf die speziellen Dedekindschen Summen sowie auf gewisse einfacher gebaute, nach Eisenstein und Stern benannte Summen zu reduzieren. Auf Grund dieser Reduktion ergibt sich ein neuer Beweis des Dieterschen Reziprozitätsgesetzes, der wesentlich auf dem einfacher zu beweisenden Dedekindschen Reziprozitätsgesetz beruht.

1. Es sei a, c ein nicht-verschwindendes, ganzzahliges, teilerfremdes Zahlenpaar. Hierzu gehört die *spezielle Dedekindsche Summe* [1], [4]

$$(1.1) \qquad s(a, c) = \sum_{\mu \bmod c}' P_1\left(\frac{a\mu}{c}\right) P_1\left(\frac{\mu}{c}\right).$$

Sie ist mittels der modulo+1 periodischen Funktion

$$(1.2) \qquad P_1(x) = x - [x] - \frac{1}{2} = R(x) - \frac{1}{2}$$

gebildet, welche das erste Bernoullische Polynom $x - \frac{1}{2}$ über das Intervall $0 \leqq x < 1$ hinaus periodisch fortsetzt. In der Definitionsformel (1.1) ist die Summation über ein volles System von Resten μ mod c unter Auslassung von Null zu erstrecken, was durch den Strich am Summenzeichen angedeutet sei.

Die wichtigste Eigenschaft der speziellen Dedekindschen Summen äußert sich darin, daß sie dem folgenden von Dedekind [1], [4] entdeckten *Reziprozitätsgesetz* genügen:

$$(1.3) \qquad \operatorname{sgn} c \cdot s(a, c) + \operatorname{sgn} a \cdot s(c, a) = \frac{a}{12c} + \frac{c}{12a} + \frac{1}{12ac} - \frac{1}{4} \operatorname{sgn}(ac).$$

Es sei wieder a, c ein wie eben beschaffenes Zahlenpaar, ferner f eine feste natürliche Zahl und g, h ein ganzzahliges Restklassenpaar modulo f. Zu diesen Gegebenheiten gehört die *allgemeine Dedekindsche Summe* [2], [3], [4]

$$(1.4) \qquad s_{gh}(a, c) = \sum_{\mu \bmod c}^{*} P_1\left(\frac{a\mu}{c} + \frac{ag + ch}{cf}\right) P_1\left(\frac{\mu}{c} + \frac{g}{cf}\right).$$

In dieser Definitionsformel ist die Summation über ein solches System von Resten μ mod c zu erstrecken, die jeweils echt-gebrochene Argumente in den beiden Faktoren liefern; dies sei durch den Stern am Summenzeichen angedeutet.

Die allgemeinen Dedekindschen Summen haben einfache formale Eigenschaften. So sind sie von dem Parameterpaar g, h wirklich nur modulo f abhängig, wie es sein muß. Und für $g = h = 0$ wird aus (1.4) der Spezialfall (1.1). Ferner ergeben sich durch Summationstransformation und unter Beachtung von $P_1(-x) = -P_1(x)$ für nicht-ganzes x die einfachen Regeln

$$(1.5) \qquad \begin{aligned} s_{gh}(a, -c) &= s_{g,-h}(a, c) = s_{-g,h}(a, c), \\ s_{gh}(-a, c) &= -s_{g,-h}(a, c) = -s_{-g,h}(a, c), \end{aligned}$$

sowie

$$(1.6) \qquad s_{gh}(a + \lambda c, c) = s_{g, \lambda g + h}(a, c) \text{ für ganzes } \lambda.$$

Die wichtigste Eigenschaft der allgemeinen Dedekindschen Summen äußert sich jedoch darin, daß sie dem folgenden von Dieter [2] entdeckten *Reziprozitätsgesetz* genügen

$$(1.7) \qquad \begin{aligned} &\operatorname{sgn} c \cdot s_{gh}(a, c) + \operatorname{sgn} a \cdot s_{hg}(c, a) \\ &= \varepsilon\left(\frac{g}{f}\right) \varepsilon\left(\frac{h}{f}\right) P_1\left(\frac{g}{f}\right) P_1\left(\frac{h}{f}\right) + \frac{1}{2}\left(\frac{a}{c} P_2\left(\frac{g}{f}\right) + \frac{1}{ac} P_2\left(\frac{ag + ch}{f}\right) + \frac{c}{a} P_2\left(\frac{h}{f}\right)\right) \\ &\qquad\qquad \text{für } g, h \not\equiv 0,\ 0 \bmod f;\ f > 1. \end{aligned}$$

Hierin ist allgemein

$$(1.8) \qquad \varepsilon(x) = \begin{cases} 0 & \text{für ganzes } x \\ 1 & \text{für nicht-ganzes } x \end{cases}$$

gesetzt. Ferner bedeutet allgemein

$$(1.\,9)\qquad P_2(x) = R^2(x) - R(x) + \frac{1}{6} = R_2(x) + \frac{1}{6}$$

diejenige modulo $+1$ periodische Funktion, welche das zweite Bernoullische Polynom $x^2 - x + \frac{1}{6}$ über das Intervall $0 \leqq x < 1$ hinaus periodisch fortsetzt.

2. Für die folgenden Entwicklungen benötigt man einige Hilfsformeln, die zunächst hergeleitet werden sollen.

Es bedeute ζ_f irgendeine primitive f-te Einheitswurzel. Dann besteht die Identität

$$(2.\,1)\qquad \sum_{\varkappa \bmod f} \frac{\zeta_f^{\varkappa} z + 1}{\zeta_f^{\varkappa} z - 1}\, \zeta_f^{-p\varkappa} = f\,\frac{z^f + 1}{z^f - 1}\, z^{\{p\}_f} - \varepsilon\left(\frac{p}{f}\right) f z^{\{p\}_f} \text{ für } z^f \neq 1,$$

wo p eine ganze Zahl ist und $\{p\}_f$ ihren kleinsten nicht-negativen Rest modulo f bezeichnet.

Zum direkten *Beweis* dieser Formel, die sich auch durch Berechnung der Koeffizienten in der an sich feststehenden Partialbruchentwicklung für die rechte Seite sofort ergibt, werde vorübergehend $|z| < 1$ angenommen. Dann ist

$$\begin{aligned}
\sum_{\varkappa \bmod f} \frac{\zeta_f^{\varkappa} z + 1}{\zeta_f^{\varkappa} z - 1}\, \zeta_f^{-p\varkappa} &= \sum_{\varkappa \bmod f} \zeta_f^{-p\varkappa} - 2 \sum_{\varkappa \bmod f} \frac{1}{1 - \zeta_f^{\varkappa} z}\, \zeta_f^{-p\varkappa} \\
&= \left(1 - \varepsilon\left(\frac{p}{f}\right)\right) f - 2 \sum_{\varkappa \bmod f} \zeta_f^{-p\varkappa} \sum_{l=0}^{\infty} (\zeta_f^{\varkappa} z)^l \\
&= \left(1 - \varepsilon\left(\frac{p}{f}\right)\right) f - 2 \sum_{l=0}^{\infty} z^l \cdot \sum_{\varkappa \bmod f} \zeta_f^{(l-p)\varkappa} \\
&= \left(1 - \varepsilon\left(\frac{p}{f}\right)\right) f - 2f \sum_{l=0}^{\infty} z^{\{p\}_f + lf} \\
&= \left(1 - \varepsilon\left(\frac{p}{f}\right)\right) f + 2f\,\frac{1}{z^f - 1}\, z^{\{p\}_f} \\
&= f\,\frac{z^f + 1}{z^f - 1}\, z^{\{p\}_f} - \varepsilon\left(\frac{p}{f}\right) f z^{\{p\}_f},
\end{aligned}$$

was nun identisch für alle z mit $z^f \neq 1$ gilt.

Ferner besteht für eine natürliche Zahl m die Entwicklung

$$(2.\,2)\qquad \frac{1}{z^m - 1} = \frac{1}{m}\,\frac{1}{z - 1} + \frac{1 - m}{2m} + \frac{m^2 - 1}{12m}(z - 1) + O\big((z - 1)^2\big) \text{ für } z^m \neq 1,$$

wo das Restglied $O\big((z-1)^2\big)$ eine bei $z = 1$ von mindestens zweiter Ordnung verschwindende rationale Funktion von z bezeichnet.

Beim *Beweis* dieser Formel handelt es sich lediglich darum, die Koeffizienten der Anfangsglieder in der an sich feststehenden Laurent-Entwicklung

$$\frac{1}{z^m - 1} = \frac{a_{-1}}{z - 1} + a_0 + a_1(z - 1) + O\big((z - 1)^2\big)$$

zu berechnen. Hier ist nun mit $g(z) = z^{m-1} + z^{m-2} + \cdots + 1$

$$a_{-1} = \frac{1}{g(1)} = \frac{1}{m},$$

$$a_0 = \frac{d}{dz}\left(\frac{1}{g(z)}\right)_{z=1} = -\frac{g'(1)}{g^2(1)} = -\frac{(m-1)+\cdots+1}{m^2} = -\frac{\binom{m}{2}}{m^2} = \frac{1-m}{2m},$$

$$a_1 = \frac{1}{2}\frac{d^2}{dz^2}\left(\frac{1}{g(z)}\right)_{z=1} = \frac{1}{2}\,\frac{-g''(1)\,g(1) + 2g'^2(1)}{g^3(1)}$$

$$= \frac{\binom{m}{2}^2 - \frac{1}{2}\left((m-1)(m-2)+\cdots+2\cdot 1\right)m}{m^3}$$

$$= \frac{\binom{m}{2}^2 - \frac{1}{2}\left(\frac{(m-1)\,m(2m-1)}{6} - \frac{(m-1)\,m}{2}\right)m}{m^3} = \frac{\binom{m}{2}^2 - \binom{m}{3}m}{m^3} = \frac{m^2-1}{12m},$$

wie in (2. 2) behauptet.

Schließlich besteht für eine natürliche Zahl n die Entwicklung

$$(2.\,3)\qquad z^n = \left(1+(z-1)\right)^n = 1 + n(z-1) + \binom{n}{2}(z-1)^2 + O\left((z-1)^3\right),$$

wo das Restglied $O\left((z-1)^3\right)$ eine bei $z=1$ von mindestens dritter Ordnung verschwindende ganze rationale Funktion von z bezeichnet.

Aus (2. 1) sowie (2. 2), (2. 3) erhält man nun durch Bildung der Differenz

$$\sum_{\varkappa \bmod f} \frac{\zeta_f^{\varkappa} z + 1}{\zeta_f^{\varkappa} z - 1}\,\zeta_f^{-p\varkappa} - \frac{z+1}{z-1}$$

und nachfolgenden Grenzübergang $z \to 1$ die Formel von Eisenstein [4]

$$(2.\,4)\qquad \frac{1}{2f}\sum_{\varkappa \bmod f}{}' \frac{\zeta_f^{\varkappa}+1}{\zeta_f^{\varkappa}-1}\,\zeta_f^{-p\varkappa} = P_1\left(\frac{p}{f}\right) \text{ für } p \not\equiv 0 \bmod f.$$

Hierdurch werden die Teilwerte der Funktion $P_1(x)$ als Interpolationswerte des trigonometrischen Polynoms

$$\frac{1}{2f}\sum_{\varkappa=1}^{f-1} \frac{e^{\frac{2\pi i}{f}\varkappa}+1}{e^{\frac{2\pi i}{f}\varkappa}-1}\,e^{-2\pi i x\varkappa}$$

dargestellt.

3. Durch Anwendung von (2. 4) mit dem Nenner cf statt f erhält man nun für die allgemeine Dedekindsche Summe in (1. 4) zunächst die Darstellung

$$(3.\,1)\qquad s_{gh}(a,c) = \frac{1}{4c^2f^2}\sum_{\mu \bmod c}{}^{*}\ \sum_{\varkappa,\lambda \bmod cf}{}' \frac{\zeta_{cf}^{\varkappa}+1}{\zeta_{cf}^{\varkappa}-1}\,\frac{\zeta_{cf}^{\lambda}+1}{\zeta_{cf}^{\lambda}-1}\,\zeta_{cf}^{-(af\mu+G)\varkappa-(f\mu+g)\lambda},$$

wo hier und im folgenden $ag + ch = G$ gesetzt ist. Zur weiteren Umgestaltung von (3. 1) hat man die Einheitswurzelsumme

$$\sum_{\mu \bmod c}{}^{*}\ \zeta_{cf}^{-(af\varkappa+f\lambda)\mu} = \sum_{\mu \bmod c}{}^{*}\ \zeta_{c}^{-(a\varkappa+\lambda)\mu}$$

zu berechnen. Nach der Bedeutung des Sterns * in der Definitionsformel (1. 4) ist offenbar

$$\sum_{\mu \bmod c}^{*} \zeta_c^{(a\varkappa+\lambda)\mu} = \begin{cases} \sum\limits_{\mu \bmod c} \zeta_c^{(a\varkappa+\lambda)\mu} - 1 & \text{für } g, h \equiv 0, 0 \bmod f, \\ \sum\limits_{\mu \bmod c} \zeta_c^{(a\varkappa+\lambda)\mu} + \left(\varepsilon\left(\frac{g}{f}\right)-1\right) + \left(\varepsilon\left(\frac{G}{f}\right)-1\right) \zeta_c^{(a\varkappa+\lambda)\mu_0} & \\ & \text{für } g, h \not\equiv 0, 0 \bmod f, \end{cases}$$

wobei sich zuletzt, falls $f \mid G$ gilt, der Ausnahmewert μ_0 aus der Kongruenz

$$a\mu_0 + \frac{G}{f} \equiv 0 \bmod c$$

bestimmt. Also ist endlich

$$\sum_{\mu \bmod c}^{*} \zeta_c^{(a\varkappa+\lambda)\mu} = \begin{cases} \left\{\begin{matrix} 0-1, \text{ wenn } a\varkappa+\lambda \not\equiv 0 \bmod c \\ |c|-1, \text{ wenn } a\varkappa+\lambda \equiv 0 \bmod c \end{matrix}\right\} & \text{für } g, h \equiv 0, 0 \bmod f, \\ \left\{\begin{matrix} 0 + \left(\varepsilon\left(\frac{g}{f}\right)-1\right) + \left(\varepsilon\left(\frac{G}{f}\right)-1\right) \zeta_c^{(a\varkappa+\lambda)\mu_0}, \text{ wenn } a\varkappa+\lambda \not\equiv 0 \bmod c \\ |c| + \left(\varepsilon\left(\frac{g}{f}\right)-1\right) + \left(\varepsilon\left(\frac{G}{f}\right)-1\right) \zeta_c^{(a\varkappa+\lambda)\mu_0}, \text{ wenn } a\varkappa+\lambda \equiv 0 \bmod c \end{matrix}\right\} & \\ & \text{für } g, h \not\equiv 0, 0 \bmod f. \end{cases}$$

Wegen

$$\sum_{\varkappa \bmod cf}' \frac{\zeta_{cf}^{\varkappa}+1}{\zeta_{cf}^{\varkappa}-1} = \sum_{\lambda \bmod cf}' \frac{\zeta_{cf}^{\lambda}+1}{\zeta_{cf}^{\lambda}-1} = 0$$

ergibt sich somit aus (3. 1) die vorläufige Formel

$$(3.\ 2) \qquad s_{gh}(a, c) = \frac{1}{4\,|c|\,f^2} \sum_{\substack{\varkappa, \lambda \bmod cf \\ a\varkappa+\lambda \equiv 0 \bmod c}}' \frac{\zeta_{cf}^{\varkappa}+1}{\zeta_{cf}^{\varkappa}-1} \frac{\zeta_{cf}^{\lambda}+1}{\zeta_{cf}^{\lambda}-1} \zeta_{cf}^{(G\varkappa+g\lambda)}.$$

Setzt man nun hierin $\varkappa = c\mu + \varrho$, $\lambda = c\nu + \sigma$ an, wo μ, ν bzw. ϱ, σ je ein volles Restsystem modulo f bzw. modulo c, etwa jeweils das kleinste solche, durchlaufen, so ist die Summationsbedingung $a\varkappa + \lambda \equiv 0 \bmod c$ mit $a\varrho + \sigma \equiv 0$, $\sigma = \sigma(\varrho) \equiv -a\varrho \bmod c$ gleichbedeutend. Hiernach wird weiter

$$(3.\ 3) \qquad s_{gh}(a, c) = \frac{1}{4\,|c|\,f^2} \sum_{\mu, \nu \bmod f} \sum_{\varrho \bmod c}' \frac{\zeta_f^{\mu}\zeta_{cf}^{\varrho}+1}{\zeta_f^{\mu}\zeta_{cf}^{\varrho}-1} \frac{\zeta_f^{\nu}\zeta_{cf}^{\sigma(\varrho)}+1}{\zeta_f^{\nu}\zeta_{cf}^{\sigma(\varrho)}-1} \zeta_f^{G\mu-g\nu} \zeta_{cf}^{G\varrho-g\sigma(\varrho)},$$

wobei der Strich am inneren Summenzeichen andeutet, daß für $\mu = 0$ oder $\nu = 0$ der Wert $\varrho = 0$, also auch $\sigma(\varrho) = 0$ auszulassen ist. Nimmt man in der Darstellung (3. 3) die von $\varrho = 0$, $\sigma(\varrho) = 0$ herrührende Teilsumme vorweg, so ist dieser Beitrag zur Dedekindschen Summe gemäß (2. 4)

$$\sum_{\mu \bmod f}' \frac{\zeta_f^{\mu}+1}{\zeta_f^{\mu}-1} \zeta_f^{G\mu} \cdot \sum_{\nu \bmod f}' \frac{\zeta_f^{\nu}+1}{\zeta_f^{\nu}-1} \zeta_f^{g\nu} = \varepsilon\left(\frac{g}{f}\right) \varepsilon\left(\frac{G}{f}\right) 4f^2 P_1\left(\frac{g}{f}\right) P_1\left(\frac{G}{f}\right).$$

Ferner ist gemäß (2. 1) für $\varrho \neq 0$, $\sigma(\varrho) \neq 0$

$$\sum_{\mu \bmod f} \frac{\zeta_f^{\mu}\zeta_{cf}^{\varrho}+1}{\zeta_f^{\mu}\zeta_{cf}^{\varrho}-1} \zeta_f^{G\mu} = f \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1} \zeta_{cf}^{\varrho\{G\}_f} - \varepsilon\left(\frac{G}{f}\right) f \zeta_{cf}^{\varrho\{G\}_f},$$

$$\sum_{\nu \bmod f} \frac{\zeta_f^{\nu}\zeta_{cf}^{\sigma(\varrho)}+1}{\zeta_f^{\nu}\zeta_{cf}^{\sigma(\varrho)}-1} \zeta_f^{g\nu} = f \frac{\zeta_c^{\sigma(\varrho)}+1}{\zeta_c^{\sigma(\varrho)}-1} \zeta_{cf}^{\sigma(\varrho)\{g\}_f} - \varepsilon\left(\frac{g}{f}\right) f \zeta_{cf}^{\sigma(\varrho)\{g\}_f}.$$

Unter Beachtung der Gleichungen $G - \{G\}_f = \left[\frac{G}{f}\right] f$, $g - \{g\}_f = \left[\frac{g}{f}\right] f$ sowie der Kongruenz $\sigma(\varrho) \equiv -a\varrho \bmod c$ ergibt sich nunmehr bei wiederholter Anwendung der Eisensteinschen Formel (2. 4) nach leichter Zwischenrechnung aus (3. 3) die endgültige Formel

$$
\begin{aligned}
(3.\,4)\qquad s_{gh}(a, c) = &-\frac{1}{4|c|} \sum_{\varrho \bmod c}{}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1} \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} \zeta_c^{-\left(\left[\frac{G}{f}\right]-\left[\frac{g}{f}\right]a\right)\varrho} \\
&+ \varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)\frac{1}{|c|} P_1\left(\frac{g}{f}\right) P_1\left(\frac{G}{f}\right) \\
&-\frac{1}{2}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\left(\left[\frac{G}{f}\right]-\left[\frac{g}{f}\right]a\right)\frac{1}{c}\right) P_1\left(\left(\left[\frac{G}{f}\right]-\left[\frac{g}{f}\right]a\right)\frac{1}{|c|}\right) \\
&+\frac{1}{2}\varepsilon\left(\frac{G}{f}\right)\varepsilon\left(\left(\left[\frac{G}{f}\right]a^{-1}-\left[\frac{g}{f}\right]\right)\frac{1}{c}\right) P_1\left(\left(\left[\frac{G}{f}\right]a^{-1}-\left[\frac{g}{f}\right]\right)\frac{1}{|c|}\right) \\
&-\frac{1}{4|c|}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)+\frac{1}{4}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)-\frac{1}{4}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)\varepsilon\left(\left(\left[\frac{G}{f}\right]-\left[\frac{g}{f}\right]a\right)\frac{1}{c}\right) \\
&\qquad \text{mit } G = ag + ch,\ aa^{-1} \equiv 1 \bmod c.
\end{aligned}
$$

Normiert man g gemäß $0 \leqq g < f$, so erhält man hieraus die einfachere Darstellung

$$
\begin{aligned}
(3.\,5)\qquad s_{gh}(a, c) = &-\frac{1}{4|c|} \sum_{\varrho \bmod c}{}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1} \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} \zeta_c^{-\left[\frac{G}{f}\right]\varrho} + \varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)\frac{1}{|c|} P_1\left(\frac{g}{f}\right) P_1\left(\frac{G}{f}\right) \\
&-\frac{1}{2}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\left[\frac{G}{f}\right]\frac{1}{c}\right) P_1\left(\left[\frac{G}{f}\right]\frac{1}{|c|}\right)+\frac{1}{2}\varepsilon\left(\frac{G}{f}\right)\varepsilon\left(\left[\frac{G}{f}\right]\frac{1}{c}\right) P_1\left(\left[\frac{G}{f}\right]\frac{a^{-1}}{|c|}\right) \\
&-\frac{1}{4|c|}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)+\frac{1}{4}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)-\frac{1}{4}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)\varepsilon\left(\left[\frac{G}{f}\right]\frac{1}{c}\right) \\
&\qquad \text{mit } G = ag + ch,\ aa^{-1} \equiv 1 \bmod c.
\end{aligned}
$$

Diese beiden Formeln (3. 4), (3. 5) sind in Hinblick auf die trigonometrische Schreibweise des Summenausdrucks

$$
\begin{aligned}
&-\frac{1}{4|c|} \sum_{\varrho \bmod c}{}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1} \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} \zeta_c^{-\left(\left[\frac{G}{f}\right]-\left[\frac{g}{f}\right]a\right)\varrho} \\
&\qquad = \frac{1}{4|c|} \sum_{\varrho \bmod c}{}' \operatorname{ctg}\frac{\pi\varrho}{c} \operatorname{ctg}\frac{\pi a\varrho}{c} \cos\frac{2\pi}{c}\left(\left[\frac{G}{f}\right]-\left[\frac{g}{f}\right]a\right)\varrho
\end{aligned}
$$

als das Analogon der Rademacherschen Cotangentenformel [6] für die speziellen Dedekindschen Summen anzusehen, in die sie in der Tat für $g \equiv h \equiv 0 \bmod f$ bzw. $g = h = 0$ übergehen. Da der vorstehende Ausdruck bei allen Automorphismen des Körpers der c-ten Einheitswurzeln invariant bleibt, ist er rational, was natürlich wegen der Rationalität von $s_{gh}(a, c)$ selbstverständlich ist. Es entsteht daher die Aufgabe, den fraglichen Summenausdruck in rationale Gestalt zu setzen.

4. Setzt man abkürzend $\left[\frac{ag+ch}{f}\right] - \left[\frac{g}{f}\right]a = \left[\frac{G}{f}\right] - \left[\frac{g}{f}\right]a = k$, so handelt es sich jetzt darum, die im Körper der c-ten Einheitswurzeln gebildete Summe

$$
(4.\,1)\qquad s_k(a, c) = -\frac{1}{4|c|} \sum_{\varrho \bmod c}{}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1} \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} \zeta_c^{-k\varrho}
$$

in rationale Gestalt überzuführen. Bezeichnet k_0 den kleinsten nicht-negativen Rest von k modulo c, so hat man im Kreiskörper zunächst die identischen Umformungen

$$\begin{aligned} s_k(a,c) &= -\frac{1}{4|c|}\sum_{\varrho \bmod c}{}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1}\frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1}(\zeta_c^{k_0\varrho}-1) - \frac{1}{4|c|}\sum_{\varrho \bmod c}{}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1}\frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} \\ &= -\frac{1}{4|c|}\sum_{\varrho \bmod c}{}' \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1}(\zeta_c^{k_0\varrho}-1) - \frac{1}{2|c|}\sum_{\varrho \bmod c}{}' \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1}\frac{\zeta_c^{k_0\varrho}-1}{\zeta_c^{\varrho}-1} \\ &\qquad - \frac{1}{4|c|}\sum_{\varrho \bmod c}{}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1}\frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} \\ &= -\frac{1}{4|c|}\sum_{\varrho \bmod c}{}' \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1}\zeta_c^{k_0\varrho} - \frac{1}{2|c|}\sum_{\varrho \bmod c}{}' \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1}(1+\zeta_c^{\varrho}+\cdots+\zeta_c^{(k_0-1)\varrho}) \\ &\qquad - \frac{1}{4|c|}\sum_{\varrho \bmod c}{}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1}\frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1}. \end{aligned}$$

Trägt man hierin für die einzelnen Summen vermöge (2. 4) und (3. 5) mit $g = h = 0$ ihre rationalen Werte ein, so erhält man die gesuchte rationale Darstellung

$$(4.\,2)\qquad s_k(a,c) = -\frac{1}{2}\varepsilon\left(\frac{k}{c}\right)P_1\left(\frac{ka^{-1}}{|c|}\right) + \sum_{\mu=1}^{\{k\}_c} P_1\left(\frac{a^{-1}\mu}{|c|}\right) + s(a,c)$$

$$\text{mit } \{k\}_c = k_0 \equiv k \bmod c,\ 0 \leqq \{k\}_c < |c|,\quad aa^{-1} \equiv 1 \bmod c,$$

die offenbar auch für $k \equiv 0 \bmod c$, $\{k\}_c = 0$ richtig ist. Damit ergibt sich endlich aus (3. 5) für die allgemeinen Dedekindschen Summen die Reduktionsformel

$$\begin{aligned} (4.\,3)\quad s_{gh}(a,c) &= s(a,c) + \sum_{\mu=1}^{\left\{\left[\frac{G}{f}\right]\right\}_c} P_1\left(\frac{a^{-1}\mu}{|c|}\right) + \varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)\frac{1}{|c|}P_1\left(\frac{g}{f}\right)P_1\left(\frac{G}{f}\right) \\ &\quad - \frac{1}{2}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\left[\frac{G}{f}\right]\frac{1}{c}\right)P_1\left(\left[\frac{G}{f}\right]\frac{1}{|c|}\right) + \frac{1}{2}\left(\varepsilon\left(\frac{G}{f}\right)-1\right)\varepsilon\left(\left[\frac{G}{f}\right]\frac{1}{c}\right)P_1\left(\left[\frac{G}{f}\right]\frac{a^{-1}}{|c|}\right) \\ &\quad + \frac{|c|-1}{4|c|}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right) - \frac{1}{4}\varepsilon\left(\frac{g}{f}\right)\varepsilon\left(\frac{G}{f}\right)\varepsilon\left(\left[\frac{G}{f}\right]\frac{1}{c}\right) \end{aligned}$$

$$\text{mit } G = ag + ch,\ 0 \leqq g < f,\ aa^{-1} \equiv 1 \bmod c.$$

Hierdurch werden die allgemeinen Dedekindschen Summen $s_{gh}(a,c)$ im wesentlichen auf die speziellen Dedekindschen Summen $s(a,c) = s_{00}(a,c)$ und auf die sogenannten *allgemeinen Eisenstein-Sternschen Summen* [4]

$$(4.\,4)\qquad t_k(d,c) = \sum_{\mu=1}^{\{k\}_c} P_1\left(\frac{d\mu}{c}\right),\ (d,c) = 1$$

zurückgeführt. Gilt insbesondere $a \equiv 1$, $c \equiv 0 \bmod f$, so nimmt die Reduktion (4. 3) die folgende einfache Gestalt an

$$(4.\,5)\qquad s_{gh}(a,c) = s(a,c) + t_k(a^{-1},|c|) - \frac{1}{2}P_1\left(\frac{k}{|c|}\right) + \frac{1}{|c|}R_2\left(\frac{g}{f}\right)$$

$$\text{mit } k = \left[\frac{G}{f}\right] = \frac{a-1}{f}g + \frac{c}{f}h;$$

diese Formel ist bereits auf andere Weise vom Verfasser [4] hergeleitet worden.

5. Auf Grund von (4. 3) ist nun der Beweis des Dieterschen Reziprozitätsgesetzes (1. 7) zunächst auf den Beweis des Dedekindschen Reziprozitätsgesetzes (1. 3) zurückgeführt. Da offenbar $s(-a,c) = -s(a,c)$ und $s(a,-c) = s(a,c)$ gilt, genügt es, das letztere Gesetz lediglich für den Spezialfall $a > 0$, $c > 0$ zu beweisen.

Sei a, c ein beliebiges positives teilerfremdes Zahlenpaar. Die Einheitswurzeldarstellung (3. 5) der zugeordneten Dedekindschen Summe $s(a, c) = s_{00}(a, c)$ läßt sich dann wie folgt zweckmäßig umformen. Es ist

$$\begin{aligned} s(a, c) &= -\frac{1}{4c} \sum_{\varrho \bmod c}' \frac{\zeta_c^{\varrho}+1}{\zeta_c^{\varrho}-1} \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} \\ &= -\frac{1}{4c} \sum_{\varrho \bmod c}' \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} - \frac{1}{2c} \sum_{\varrho \bmod c}' \frac{1}{\zeta_c^{\varrho}-1} \frac{\zeta_c^{a\varrho}+1}{\zeta_c^{a\varrho}-1} \\ &= \frac{1}{2c} \sum_{\varrho \bmod c}' \frac{1}{1-\zeta_c^{\varrho}} - \frac{1}{c} \sum_{\varrho \bmod c}' \frac{1}{(1-\zeta_c^{\varrho})(1-\zeta_c^{a\varrho})}. \end{aligned}$$

Hierin ist

$$\sum_{\varrho \bmod c}' \frac{1}{1-\zeta_c^{\varrho}} = -\sum_{\varrho \bmod c}' \frac{\zeta_c^{\varrho}}{1-\zeta_c^{\varrho}} = \frac{1}{2} \sum_{\varrho \bmod c}' 1 = \frac{c-1}{2}.$$

Also hat man

$$s(a, c) = \frac{c-1}{4c} - \frac{1}{c} \sum_{\varrho \bmod c}' \frac{1}{(1-\zeta_c^{\varrho})(1-\zeta_c^{a\varrho})}. \tag{5. 1}$$

Man führe nunmehr in naheliegender Weise die für $|z| < 1$ holomorphe rationale Funktion

$$h(z) = \sum_{\varrho \bmod c} \frac{1}{(1-\zeta_c^{\varrho} z)(1-\zeta_c^{a\varrho} z^a)} \tag{5. 2}$$

ein. Durch Entwicklung in Potenzreihen erhält man hierfür zunächst

$$\begin{aligned} h(z) &= \sum_{\varrho \bmod c} \left(\sum_{m=0}^{\infty} (\zeta_c^{\varrho} z)^m \right) \left(\sum_{n=0}^{\infty} (\zeta_c^{a\varrho} z^a)^n \right) \\ &= \sum_{\varrho \bmod c} 1 + \sum_{m=1}^{\infty} z^m \left(\sum_{\varrho \bmod c} \zeta_c^{\varrho m} \right) + \sum_{n=1}^{\infty} z^{an} \left(\sum_{\varrho \bmod c} \zeta_c^{a\varrho n} \right) + \sum_{m,n=1}^{\infty} z^{m+an} \left(\sum_{\varrho \bmod c} \zeta_c^{(m+an)\varrho} \right). \end{aligned}$$

Trägt man für die vortretenden Einheitswurzelsummen ihre Werte ein, so wird weiter

$$h(z) = c + c \sum_{m=1}^{\infty} z^{cm} + c \sum_{n=1}^{\infty} z^{acn} + c \sum_{r=1}^{\infty} z^{cr} \left(\sum_{\substack{m+an=cr \\ m,n \geqq 1}} 1 \right).$$

Für die Lösungsanzahl der diophantischen Gleichung $m + an = cr$ bei festem $r \geqq 1$ erhält man nun durch Abzählen die Formeln

$$\sum_{\substack{m+an=cr \\ m,n \geqq 1}} 1 = \begin{cases} \left[\dfrac{cr}{a}\right] & \text{für } a \nmid r \\ \left[\dfrac{cr}{a}\right] - 1 & \text{für } a \mid r. \end{cases}$$

Hierdurch wird

$$h(z) = c + c \sum_{m=1}^{\infty} z^{cm} + c \sum_{r=1}^{\infty} \left[\frac{cr}{a}\right] z^{cr}.$$

Führt man hierin statt der nicht-periodischen Funktion $[x]$ die modulo$^+1$ periodische Funktion $P_1(x)$ aus (1. 2) ein, so ist auch

$$h(z) = c + c \sum_{m=1}^{\infty} z^{cm} + \frac{c^2}{a} \sum_{r=1}^{\infty} r z^{cr} - \frac{c}{2} \sum_{r=1}^{\infty} z^{cr} - c \sum_{\varrho=0}^{a-1} P_1\left(\frac{c\varrho}{a}\right) \sum_{r=0}^{\infty} z^{acr+c\varrho} - \frac{c}{2}.$$

Stellt man schließlich die auftretenden geometrischen bzw. abgeleiteten geometrischen Reihen in geschlossener Form dar, so erhält man wegen $\sum_{\varrho=1}^{a-1} P_1\left(\frac{c\varrho}{a}\right) = 0$ nach leichter Zwischenrechnung die Endformel

$$(5.3)\quad h(z) = \left(\frac{c^2}{a} - \frac{c}{2}\right)\frac{1}{z^c - 1} - \frac{c}{2}\,\frac{1}{z^{ac}-1} + \frac{c^2}{a}\,\frac{1}{(z^c-1)^2} + c\sum_{\varrho=1}^{a-1} P_1\left(\frac{c\varrho}{a}\right)\frac{z^{c\varrho}-1}{z^{ac}-1}.$$

Entwickelt man in dieser Identität die einzelnen Glieder der rechten Seite gemäß (2. 2), so fallen in der Differenz $h(z) - \frac{1}{(z-1)(z^a-1)}$ die polaren Bestandteile heraus, wie es sein muß, und man erhält hierfür die Näherungsformel

$$(5.4)\quad \sum_{\varrho \bmod c}{}' \frac{1}{(1-\zeta_c^{\varrho} z)(1-\zeta_c^{a\varrho} z^a)} = \frac{6ac - a^2 - c^2 - 3a - 1}{12a} + c\sum_{\varrho=1}^{a-1} P_1\left(\frac{c\varrho}{a}\right)\frac{\varrho}{a} + O(z-1),$$

wo das Restglied $O(z-1)$ eine bei $z=1$ verschwindende rationale Funktion von z bezeichnet. Hierin ist nun

$$\sum_{\varrho=1}^{a-1} P_1\left(\frac{c\varrho}{a}\right)\frac{\varrho}{a} = \sum_{\varrho \bmod a}{}' P_1\left(\frac{c\varrho}{a}\right) P_1\left(\frac{\varrho}{a}\right) = s(c, a).$$

Damit ergibt sich endlich aus (5. 1), (5, 2), (5. 4)

$$(5.5)\qquad s(a, c) + s(c, a) = \frac{a}{12c} + \frac{c}{12a} + \frac{1}{12ac} - \frac{1}{4}.$$

Dieses ist die Dedekindsche Reziprozitätsformel (1. 3) für die speziellen Dedekindschen Summen.

6. Für den endgültigen Beweis von (1. 7) kommt es im Hinblick auf die Reduktion (4. 3) wesentlich nur noch auf die Berechnung der Summe

$$(6.1)\qquad t_k(a^{-1}, |c|) + t_k(c^{-1}, |a|) = \sum_{\mu=1}^{\{k\}_c} P_1\left(\frac{a^{-1}\mu}{|c|}\right) + \sum_{\nu=1}^{\{k\}_a} P_1\left(\frac{c^{-1}\nu}{|a|}\right)$$
$$\text{mit } k = \left[\frac{G}{f}\right] = \left[\frac{ag+ch}{f}\right]$$

an. Auf Grund der einfachen Regeln (1. 5) kann man sich beim Beweis von (1. 7) und also auch bei der Berechnung von (6. 1) auf positive a und c beschränken. Neben den Normierungen $0 \leqq g < f$, $0 \leqq h < f$ sei schließlich noch ohne Einschränkung $a \leqq c$ angenommen, mit Gleichheit nur für $a = c = 1$. In (6. 1) sind a^{-1} und c^{-1} in ihren primen Restklassen modulo c bzw. modulo a noch beliebig wählbar. Man binde sie durch die Gleichung $aa^{-1} + cc^{-1} = 1$ und wähle überdies $a^{-1} > 0$, dann ist wegen $a > 0$, $c > 0$ notwendig $c^{-1} < 0$. Nun ist $k = \left[\frac{k}{c}\right] c + \{k\}_c$ und hierbei gilt auf Grund der getroffenen Normierungen

$$0 \leqq \left[\frac{k}{c}\right] = \left[\left[\frac{ag+ch}{f}\right]\frac{1}{c}\right] \leqq \left[\frac{ag+ch}{f}\right]\frac{1}{c} \leqq \frac{g+h}{f} < 2,$$

so daß für die obere Summationsgrenze $\{k\}_c$ der ersteren Summe in (6. 1) nur die Werte $\{k\}_c = k$ oder $\{k\}_c = k - c$ in Betracht kommen.

Sei zunächst $\left[\frac{k}{c}\right] = 0$, also $0 \leqq \{k\}_c = k < c$. Dann wird wegen $aa^{-1} + cc^{-1} = 1$

$$\begin{aligned} t_k(a^{-1}, c) &= \sum_{\mu=1}^{k} P_1\left(\frac{a^{-1}\mu}{c}\right) = \sum_{\mu=1}^{k} P_1\left(\frac{\mu}{ac} - \frac{c^{-1}\mu}{a}\right) \\ &= \sum_{\mu=1}^{k} \frac{\mu}{ac} + \sum_{\mu=1}^{k} P_1\left(-\frac{c^{-1}\mu}{a}\right) \\ &= \frac{k(k+1)}{2ac} - \sum_{\mu=1}^{\{k\}_a} P_1\left(\frac{c^{-1}\mu}{a}\right) - \frac{1}{2}\left[\frac{k}{a}\right]. \end{aligned}$$

Also hat man in diesem Fall für (6. 1) den expliziten Wert

$$(6.\ 2) \qquad t_k(a^{-1}, c) + t_k(c^{-1}, a) = \frac{1}{2ac}(k^2 + k) - \frac{1}{2}\left[\frac{k}{a}\right] \text{ mit } k = \left[\frac{ag + ch}{f}\right],$$

der von der Wahl von a^{-1} und c^{-1} aus ihren Restklassen modulo c bzw. modulo a unabhängig ist, wie es sein muß.

Ist dagegen $\left[\frac{k}{c}\right] = 1$, also $0 \leqq \{k\}_c = k - c$, so ergibt sich ähnlich wie eben für (6. 1) der explizite Wert

$$(6.\ 3) \qquad t_k(a^{-1}, c) + t_k(c^{-1}, a) = \frac{1}{2ac}(k^2 + k) - \frac{1}{2}\left[\frac{k}{a}\right] - \frac{1}{2} \text{ mit } k = \left[\frac{ag + ch}{f}\right].$$

Durch die Formeln (5. 5), (6. 2) bzw. (6. 3) sind nunmehr alle wesentlichen Hilfsmittel bereitgestellt, um die Dietersche Reziprozitätsformel (1. 7) für die allgemeinen Dedekindschen Summen auf Grund ihrer Reduktion (4. 3) vollständig zu beweisen. Hierfür sind nur noch ganz elementare Rechnungen durchzuführen, die lediglich den Charakter einer Verifikation der rechten Seite von (1. 7) haben. Es mag daher genügen, die fraglichen Ausrechnungen für die beiden wichtigsten Fälle wirklich auszuführen.

Sei $g \neq 0$, $h \neq 0$ und $\frac{G}{f} = \frac{ag + ch}{f}$ ganz, also $k = \left[\frac{G}{f}\right] = \frac{G}{f}$. Auf Grund von (4. 3) sowie (5. 5), (6. 2), (6. 3) ist dann zunächst für $a \nmid k$, $c \nmid k$, mit $aa^{-1} + cc^{-1} = 1$

$$\begin{aligned} s_{gh}(a, h) + s_{hg}(c, a) &= \frac{a}{12c} + \frac{c}{12a} + \frac{1}{12ac} - \frac{1}{4} + \frac{1}{2ac}\left(\frac{G^2}{f^2} + \frac{G}{f}\right) - \frac{1}{2}\left[\frac{G}{af}\right[- \frac{1}{2}\left[\frac{G}{cf}\right] \\ &\quad - \frac{1}{2} P_1\left(\frac{G}{cf}\right) - \frac{1}{2} P_1\left(\frac{Ga^{-1}}{cf}\right) - \frac{1}{2} P_1\left(\frac{G}{af}\right) - \frac{1}{2} P_1\left(\frac{Gc^{-1}}{af}\right) \\ &= \frac{a}{12c} + \frac{c}{12a} + \frac{1}{12ac} + \frac{1}{4} + \frac{1}{2ac}\frac{G^2}{f^2} - \frac{1}{2}\frac{G}{af} - \frac{1}{2}\frac{G}{cf}, \end{aligned}$$

und diese letzte Umformung gilt auch für $a \mid k$ oder $c \mid k$. Somit ergibt sich im vorliegenden Falle in abgekürzter Form

$$s_{gh}(a, c) + s_{hg}(c, a) = P_1\left(\frac{g}{f}\right) P_1\left(\frac{h}{f}\right) + \frac{1}{2}\left(\frac{a}{c} P_2\left(\frac{g}{f}\right) + \frac{1}{ac} P_2(0) + \frac{c}{a} P_2\left(\frac{h}{f}\right)\right),$$

das ist (1. 7).

Sei $g \neq 0$, $h \neq 0$ und $\frac{G}{f} = \frac{ag + ch}{f}$ nicht-ganz. Auf Grund von (4. 3) sowie (5. 5), (6. 2), (6. 3) ist dann zunächst für $a \nmid k$, $c \nmid k$, mit $[x] = x - R(x)$

$$
\begin{aligned}
s_{gh}(a, c) + s_{hg}(c, a) = {} & \frac{a}{12c} + \frac{c}{12a} + \frac{1}{12ac} \\
& - \frac{1}{4} + \frac{1}{2ac}\left(\frac{G^2}{f^2} - 2\frac{G}{f} R\left(\frac{G}{f}\right) + R^2\left(\frac{G}{f}\right) + \frac{G}{f} - R\left(\frac{G}{f}\right)\right) \\
& - \frac{1}{2}\left[\left[\frac{G}{f}\right]\frac{1}{a}\right] - \frac{1}{2}\left[\left[\frac{G}{f}\right]\frac{1}{c}\right] + P_1\left(\frac{G}{f}\right)\left(\frac{1}{c} P_1\left(\frac{g}{f}\right) + \frac{1}{a} P_1\left(\frac{h}{f}\right)\right) \\
& - \frac{1}{2} P_1\left(\left[\frac{G}{f}\right]\frac{1}{c}\right) - \frac{1}{2} P_1\left(\left[\frac{G}{f}\right]\frac{1}{a}\right) - \frac{1}{4c} - \frac{1}{4a} \\
= {} & \frac{a}{12c} + \frac{c}{12a} + \frac{1}{12ac} + \frac{1}{4} + \frac{1}{2ac}\frac{G^2}{f^2} \\
& + \frac{1}{2ac}\left(R^2\left(\frac{G}{f}\right) - R\left(\frac{G}{f}\right)\right) - \frac{1}{2}\frac{G}{af} - \frac{1}{2}\frac{G}{cf},
\end{aligned}
$$

und diese letzte Umformung gilt auch für $a \mid k$ oder $c \mid k$. Somit ergibt sich im vorliegenden Falle in abgekürzter Form

$$
s_{gh}(a, c) + s_{hg}(c, a) = P_1\left(\frac{g}{f}\right) P_1\left(\frac{h}{f}\right) + \frac{1}{2}\left(\frac{a}{c} P_2\left(\frac{g}{f}\right) + \frac{1}{ac} P_2\left(\frac{ag + ch}{f}\right) + \frac{c}{a} P_2\left(\frac{h}{f}\right)\right),
$$

das ist (1. 7).

Ist $g = 0$ oder $h = 0$, so verlaufen die entsprechenden Beweise von (1. 7) noch einfacher, und der Fall negativer a oder c schließlich erledigt sich unmittelbar auf Grund von (1. 5).

Literaturverzeichnis.

[1] *R. Dedekind*, Erläuterungen zu den vorstehenden Fragmenten (zu B. Riemann, Fragmente über die Grenzfälle der elliptischen Modulfunktionen). Riemanns Werke, 2. Aufl., 466—478 = Dedekinds Werke **1**, 159—172.

[2] *U. Dieter*, Das Verhalten der Kleinschen Funktionen $\log \sigma_{g,h}(\omega_1, \omega_2)$ gegenüber Modultransformationen und verallgemeinerte Dedekindsche Summen. Journ. f. d. reine u. angew. Math. **201** (1959), 37—70.

[3] *C. Meyer*, Die Berechnung der Klassenzahl abelscher Körper über quadratischen Zahlkörpern. Berlin 1957.

[4] *C. Meyer*, Über einige Anwendungen Dedekindscher Summen. Journ. f. d. reine u. angew. Math. **198** (1957), 143—203.

[5] *H. Rademacher*, Zur Theorie der Dedekindschen Summen. Math. Zeitschr. **63** (1956), 445—463.

[6] *H. Rademacher*, Über eine Reziprozitätsformel aus der Theorie der Modulfunktionen (ungarisch mit deutschem Auszug). Matematikai és Fizikai Lapok, **40** (1933), 24—34.

Eingegangen 6. Januar 1960.

Eine Verallgemeinerung des Basisbegriffes in der additiven Zahlentheorie.

Von *Erich Härtter* in Mainz.

§ 1. Einleitung und Definitionen.

1. Ein Bestreben in der neueren additiven Zahlentheorie besteht darin, an Stelle der Menge der natürlichen Zahlen beliebige Mengen addierbarer Größen (z. B. Vektoren mit nichtnegativen ganzzahligen Komponenten) zu betrachten und Analoga zu bereits bekannten Aussagen über natürliche Zahlen zu gewinnen. Bei der Übertragung des Mannschen Satzes auf Mengen mit einfacher Komposition (Halbgruppen) sind Arbeiten von v. d. Corput-Kemperman sowie M. Kneser zu nennen. F. Kasch untersucht wesentliche Komponenten in der Menge der Vektoren mit nichtnegativen ganzzahligen Komponenten und erhält entsprechende Aussagen zu den Ergebnissen von Erdös, Brauer, Selberg u. a.

Wir wollen hier für den Basisbegriff eine abstrakte Menge mit einfacher Komposition zu Grunde legen. Man denke etwa an eine Halbgruppe. Es wird sich dann zeigen, daß eine ganze Reihe von Aussagen über Basen auch in dieser Allgemeinheit ihre Gültigkeit behalten.

Eine Menge $\mathfrak{B}$ nichtnegativer ganzer Zahlen heißt bekanntlich Basis der Ordnung h für die Menge $\mathfrak{M}$ $(0 \in \mathfrak{M})$ nichtnegativer ganzer Zahlen, wenn $h\mathfrak{B} \geqq \mathfrak{M}$ ist. Diesen Basisbegriff wollen wir in zweifacher Hinsicht verallgemeinern, indem wir

(A) an Stelle von Mengen nichtnegativer ganzer Zahlen Untermengen einer Menge $\mathfrak{G}$ mit einfacher Komposition und

(B) nicht h-mal die gleiche Menge als Basis addieren, sondern die Summe von h (nicht notwendig gleichen) Mengen zur Darstellung von $\mathfrak{M}$ betrachten. Ein solches h-Tupel von Mengen nennen wir dann Basissystem für $\mathfrak{M}$.

Für den Fall, daß $\mathfrak{G}$ die Menge $\mathfrak{Z}$ der nichtnegativen ganzen Zahlen ist und daß in den Basissystemen alle Mengen gleich sind, umfassen die allgemeinen Aussagen einige schon bekannte Resultate. Diese Sätze gelten aber auch in anderen Bereichen, wie z. B. in der Menge aller r-dimensionalen Vektoren mit ganzzahligen nichtnegativen Komponenten oder in der Menge aller nichtnegativen rationalen Zahlen (vgl. Nr. 17).

2. *Definitionen zur Verallgemeinerung* (A). Sei $\mathfrak{G}$ eine nichtleere Menge mit folgender Eigenschaft: Zu gewissen n-Tupeln $\{a_1, \ldots, a_n\}$ von Elementen aus $\mathfrak{G}$ $(1 \leqq n < \infty)$ sei eine eindeutige (Skalar-)Funktion

$$\sigma(a_1, \ldots, a_n) = c \text{ mit } c \in \mathfrak{G} \tag{1}$$

und

$$\sigma(a) = a \text{ für alle } a \in \mathfrak{G}, \tag{2}$$

die wir *Summe* nennen, erklärt[1]). Wenn $\sigma(a_1, \ldots, a_n)$ nicht erklärt ist, schreiben wir $\sigma(a_1, \ldots, a_n) = \omega$.

Wir kürzen ein n-Tupel $\{a_1, \ldots, a_n\}$ ab durch $\mathfrak{a}$ und nennen a_ν $(\nu = 1, \ldots, n)$ die Komponente von $\mathfrak{a}$. Dann schreiben wir an Stelle von (1) auch

$$\sigma(\mathfrak{a}) = c \ (c \in \mathfrak{G}) \text{ bzw. } \sigma(\mathfrak{a}) = \omega. \tag{3}$$

Ferner bezeichnen wir die Gesamtheit aller n-Tupel $\{a_1, \ldots, a_n\}$ $(1 \leqq n < \infty)$ von Elementen a_ν aus $\mathfrak{G}$ mit Γ_n und setzen $\bigcup_{n=1}^{\infty} \Gamma_n = \Gamma$. Also wäre $\Gamma_1 = \mathfrak{G}$.

Wir definieren ferner ein Element O mit der Eigenschaft

$$\begin{cases} \sigma(a_1, \ldots, a_\nu, O, a_{\nu+1}, \ldots, a_n) = \sigma(a_1, \ldots, a_\nu, a_{\nu+1}, \ldots, a_n) & (\nu = 1, \ldots, n-1), \\ \sigma(O, a_1, \ldots, a_n) = \sigma(a_1, \ldots, a_n, O) = \sigma(a_1, \ldots, a_n) \text{ für alle } \mathfrak{a} \in \Gamma \text{ und } \sigma(O) = O. \end{cases} \tag{4}$$

Weiterhin nehmen wir an, daß $\mathfrak{G}$ mindestens ein solches Element O enthält. Man überlegt sich leicht, daß dieses eindeutig bestimmt ist; denn angenommen, die Elemente O und $O^* \in \mathfrak{G}$ erfüllten die Bedingungen (4). Dann wäre $\sigma(O, O^*) = O$ und $\sigma(O, O^*) = O^*$, also $O = O^*$.

Für eine unendliche Folge $\{a_1, \ldots, a_n, \ldots\}$ von Elementen aus $\mathfrak{G}$ definieren wir die zugehörige charakteristische Folge $\{\varepsilon_1, \ldots, \varepsilon_n, \ldots\}$ ganzer Zahlen durch

$$\varepsilon_n = \begin{cases} 0, \text{ wenn } a_n = O \\ 1, \text{ wenn } a_n \neq O. \end{cases}$$

Im Fall $\sum_{\nu=1}^{\infty} \varepsilon_\nu < \infty$ setzen wir $\sigma(a_1, \ldots, a_n, \ldots) = \sigma(a_1, a_2, \ldots, a_N)$, wenn $\varepsilon_n = 0$ ist für alle $n > N \geqq 1$. Für $\sum_{\nu=1}^{\infty} \varepsilon_\nu = \infty$ ist $\sigma(a_1, \ldots, a_n, \ldots)$ nicht definiert und wir schreiben dann auch $\sigma(a_1, \ldots, a_n, \ldots) = \omega$.

Gilt insbesondere für *jedes* $\mathfrak{a} \in \Gamma$

$$\sigma(\mathfrak{a}) = \sigma(\mathfrak{a}^*),$$

wobei $\mathfrak{a}^*$ aus $\mathfrak{a}$ durch eine beliebige Permutation der Komponenten von $\mathfrak{a}$ hervorgeht, so nennen wir $\mathfrak{G}$ *kommutativ* bezüglich der Summe, andernfalls nichtkommutativ.

Besteht für jedes n-Tupel $\{a_1, \ldots, a_n\} \in \Gamma$ die Beziehung

$$\begin{aligned} \sigma(a_1, \ldots, a_n) &= \sigma(\sigma(a_1, \ldots, a_\nu), a_{\nu+1}, \ldots, a_n) \\ &= \sigma(a_1, \ldots, a_\nu, \sigma(a_{\nu+1}, \ldots, a_n)) \\ &= \sigma(\sigma(a_1, \ldots, a_\nu), \sigma(a_{\nu+1}, \ldots, a_n)) \end{aligned}$$

für alle ν mit $1 \leqq \nu \leqq n-1$, dann heißt $\mathfrak{G}$ *assoziativ* hinsichtlich der Summe.

Setzen wir $\mathfrak{G}$ assoziativ und $\sigma(\mathfrak{a}) \neq \omega$ für jedes $\mathfrak{a} \in \Gamma$ voraus, dann läßt sich $\mathfrak{G}$ als Halbgruppe mit Nullelement auffassen, wie man sich sofort überzeugt. Für die Ordnung hat man in der Halbgruppe entsprechend die Eigenschaften (12) bis (15) zu nehmen, wobei es jedoch ausreicht, (15) für binäre Verknüpfungen zu formulieren.

3. In der Menge $\mathfrak{G}$ definieren wir die Addition von Mengen:

Definition 1. *Seien* $\mathfrak{A}_\nu \leqq \mathfrak{G}$ $(\nu = 1, \ldots, n)$. *Dann verstehen wir unter der Summe* $\sum_{\nu=1}^{n} \mathfrak{A}_\nu$ *dieser Mengen (wir schreiben auch* $\mathfrak{A}_1 \otimes \cdots \otimes \mathfrak{A}_n$*) die Gesamtheit aller Elemente* $\sigma(a_1, \ldots, a_n)$ $(a_\nu \in \mathfrak{A}_\nu,\ \nu = 1, \ldots, n)$ *aus* $\mathfrak{G}$ *mit* $\sigma(a_1, \ldots, a_n) \neq \omega$.

[1]) v. d. Corput-Kemperman [2] nennen eine solche Verknüpfung partielle Addition.

Auch für unendlich viele Mengen $\mathfrak{A}_\nu \leqq \mathfrak{G}$ definieren wir eine Summe:

Definition 1'. *Seien* $\mathfrak{A}_\nu \in \mathfrak{G}$ $(\nu = 1, 2, \ldots)$ *mit* $O \in \bigcap_{\nu=1}^{\infty} \mathfrak{A}_\nu$. *Dann verstehen wir unter der Summe* $\sum_{\nu=1}^{\infty} \mathfrak{A}_\nu$ *dieser Mengen die Gesamtheit aller Elemente* $\sigma(a_1, a_2, \ldots)$ $(a_\nu \in \mathfrak{A}_\nu)$ *aus* $\mathfrak{G}$ *mit* $\sigma(a_1, a_2, \ldots) \neq \omega$.

Offenbar gilt dann $\sum_{\nu=1}^{n} \mathfrak{A}_\nu \leqq \mathfrak{G}$ bzw. $\sum_{\nu=1}^{\infty} \mathfrak{A}_\nu \leqq \mathfrak{G}$. Im Sonderfall $\mathfrak{A}_\nu = \mathfrak{A}$ $(\nu = 1, 2, \ldots, n)$ schreiben wir an Stelle von $\sum_{\nu=1}^{n} \mathfrak{A}$ auch $n\mathfrak{A}$ $(1 \leqq n \leqq \infty)$. Ist $\mathfrak{G}$ kommutativ und assoziativ, so ist auch $\sum_{\nu=1}^{n} \mathfrak{A}_\nu$ kommutativ bzw. assoziativ.

Als einfache Folgerungen ergeben sich aus diesen Definitionen $(1 \leqq n \leqq \infty)$

$$\mathfrak{A}_i \leqq \sum_{\nu=1}^{n} \mathfrak{A}_\nu, \quad \textit{falls } O \in \bigcap_{\substack{\nu=1 \\ \nu \neq i}}^{n} \mathfrak{A}_\nu \qquad (i = 1, \ldots, n); \tag{5}$$

$$\bigcup_{\nu=1}^{n} \mathfrak{A}_\nu \leqq \sum_{\nu=1}^{n} \mathfrak{A}_\nu, \quad \textit{falls } O \in \bigcap_{\nu=1}^{n} \mathfrak{A}_\nu; \tag{6}$$

$$\sum_{\substack{\nu=1 \\ \nu \neq i}}^{n} \mathfrak{A}_\nu \leqq \sum_{\nu=1}^{n} \mathfrak{A}_\nu, \quad \textit{falls } O \in \mathfrak{A}_i. \tag{7}$$

Als Spezialfall von (7) haben wir

$$n_1\mathfrak{A} \geqq n_2\mathfrak{A}, \quad \textit{wenn } n_1 \geqq n_2 \textit{ und } O \in \mathfrak{A} \textit{ ist.} \tag{8}$$

Ferner gilt

$$\sum_{\nu=1}^{n} \mathfrak{A}_\nu^* \leqq \sum_{\nu=1}^{n} \mathfrak{A}_\nu, \quad \textit{falls } \mathfrak{A}_\nu^* \leqq \mathfrak{A}_\nu \qquad (\nu = 1, \ldots, n). \tag{9}$$

Auch der Begriff der Besicovitch-Summe läßt sich auf diesen allgemeinen Fall übertragen:

Definition 2. *Seien* $\mathfrak{A}, \mathfrak{B} \leqq \mathfrak{G}$. *Unter der Besicovitch-Summe* $\mathfrak{A} \dot{\otimes} \mathfrak{B}$ *von* $\mathfrak{A}$ *und* $\mathfrak{B}$ *versteht man die Menge* $\{\mathfrak{A} \cap \{\mathfrak{G} - \{O\}\}\} \otimes \{\mathfrak{B} \cup \{O\}\}$, *wobei* $\mathfrak{G} - \{O\}$ *die Menge* $\mathfrak{G}$ *ohne das Element* O *bedeutet.*

Als Analogon zu (5) läßt sich hier zeigen

$$\mathfrak{A} \cap \{\mathfrak{G} - \{O\}\} \leqq \mathfrak{A} \dot{\otimes} \mathfrak{B}. \tag{10}$$

Wir werden jedoch weiterhin nur den Summenbegriff der Definition 1 bzw. 1' betrachten.

4. Nun kommen wir zur Verallgemeinerung (B). Zunächst definieren wir den Begriff des Basissystems:

Definition 3. *Sei* $\mathfrak{M} \leqq \mathfrak{G}$ *mit* $O \in \mathfrak{M}$. *Ein System (h-Tupel)* $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ *von h Mengen* $\mathfrak{B}_\eta \leqq \mathfrak{G}$ $(\eta = 1, \ldots, h;\ 1 \leqq h \leqq \infty)$ *mit* $O \in \bigcap_{\eta=1}^{h} \mathfrak{B}_\eta$ *heißt Basissystem der Ordnung h für* $\mathfrak{M}$, *wenn* $\sum_{\eta=1}^{h} \mathfrak{B}_\eta \geqq \mathfrak{M}$ *gilt.*

Dabei ist für $h = \infty$ das System $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ als unendliche Folge zu verstehen. Ist $h < \infty$, so sprechen wir von einem Basissystem der endlichen Ordnung h, sonst von einem Basissystem unendlicher Ordnung.

Mit anderen Worten besagt also Definition 3, daß jedes $x \in \mathfrak{M}$ als $x = \sigma(b_1, \ldots, b_h)$ $(b_\eta \in \mathfrak{B}_\eta)$ darstellbar ist, wobei auch wieder für $h = \infty$ die Folge $b_1, \ldots, b_h$ als unendliche Folge zu verstehen ist. Im Sonderfall $\mathfrak{B}_\eta = \mathfrak{B}$ $(\eta = 1, \ldots, h)$ kommen wir zum gewöhnlichen Basisbegriff:

Definition 4. *Sei $\mathfrak{M} \leqq \mathfrak{G}$ mit $O \in \mathfrak{M}$. Eine Menge $\mathfrak{B} \leqq \mathfrak{G}$ mit $O \in \mathfrak{B}$ heißt Basis für $\mathfrak{M}$, wenn sich jedes $x \in \mathfrak{M}$ in der Form $x = \sigma(b_1, \ldots, b_n)$ $(b_\nu \in \mathfrak{B};\ \nu = 1, \ldots, n;\ n = n(x) < \infty)$ darstellen läßt.*

Ist $l(x)$ die Minimalanzahl von Elementen $b_\nu \in \mathfrak{B}$, die zur Darstellung von $x \in \mathfrak{M}$ als $x = \sigma(b_1, \ldots, b_n)$ notwendig ist, so setzen wir $\overline{\operatorname{fin}}_{x \in \mathfrak{M}}\, l(x) = h_{\mathfrak{B}, \mathfrak{M}}$, wobei für $h_{\mathfrak{B}, \mathfrak{M}}$ auch der Wert ∞ zugelassen wird. Im Fall $h_{\mathfrak{B}, \mathfrak{M}} = \infty$ nennen wir $\mathfrak{B}$ eine *Basis unendlicher Ordnung für $\mathfrak{M}$* und für $h_{\mathfrak{B}, \mathfrak{M}} \leqq h$ (h natürliche Zahl) sprechen wir von einer *Basis der (endlichen) Ordnung h für $\mathfrak{M}$.*

Auf Grund von Nr. 3 können wir also schreiben $h\mathfrak{B} \geqq \mathfrak{M}$. Die Zahl $h_{\mathfrak{B}, \mathfrak{M}}$ soll die *genaue Ordnung von $\mathfrak{B}$* bezüglich $\mathfrak{M}$ heißen.

Als Zusatzbedingung kann man für die in Definition 3 erklärten Basissysteme $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ bzw. für die in Definition 4 erklärten Basen $\mathfrak{B}$ noch verlangen

$$\bigcup_{\eta=1}^{h} \mathfrak{B}_\eta \leqq \mathfrak{M} \quad \text{bzw.} \quad \mathfrak{B} \leqq \mathfrak{M}. \tag{11}$$

Obwohl manche Sätze auch mit dieser Zusatzbedingung gelten, wollen wir bei der Formulierung der Aussagen auf eine besondere Erwähnung dieser Tatsache im allgemeinen verzichten.

Die Existenz von Basissystemen bzw. Basen einer Ordnung h ist für jede Menge $\mathfrak{M}$ klar, denn man braucht ja nur $\mathfrak{B}_\eta = \mathfrak{M}$ $(\eta = 1, \ldots, h)$ bzw. $\mathfrak{B} = \mathfrak{M}$ zu setzen[2]). Von den Mengen $\mathfrak{B}_\eta$ eines Basissystems B der endlichen Ordnung h können einige endlich sein, jedoch muß, wenn $\mathfrak{M}$ unendlich ist, mindestens eine unendlich sein. Für Basen $\mathfrak{B}$ der endlichen Ordnung h im gewöhnlichen Sinn ist, wenn $\mathfrak{M}$ unendlich ist, offenbar auch $\mathfrak{B}$ unendlich.

Indem man aus den Mengen $\mathfrak{B}_\eta$ des Basissystems $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ h-ter Ordnung für $\mathfrak{M}$ die Vereinigungsmenge $\widetilde{\mathfrak{B}} = \bigcup_{\eta=1}^{h} \mathfrak{B}_\eta$ bildet, erhält man eine Basis der Ordnung h für $\mathfrak{M}$. Stöhr [14] und Raikov [9] benutzten dieses Verfahren, um mit Hilfe von Ziffern-darstellungen eine Basis $\mathfrak{B}$ h-ter Ordnung für die Menge $\mathfrak{Z}$ der nichtnegativen ganzen Zahlen mit der Anzahlfunktion[3]) $\mathfrak{B}(\|x\|) = \mathfrak{B}(x) = O\left(\sqrt[h]{x}\right)$ zu konstruieren. Umgekehrt läßt sich aus einer Basis $\mathfrak{B}$ der Ordnung h für $\mathfrak{M}$ durch $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ mit $\mathfrak{B}_1 = \cdots = \mathfrak{B}_h = \mathfrak{B}$ ein Basissystem der Ordnung h für $\mathfrak{M}$ bilden.

Volkmann [17] benutzt Basissysteme für die Menge $\mathfrak{Z}$ der nichtnegativen ganzen Zahlen, um Basen für die Menge $\mathfrak{Z}_r$ der r-dimensionalen Vektoren mit ganzzahligen nichtnegativen Komponenten zu konstruieren. Sind nämlich $B^{(\varrho)} = \{\mathfrak{B}_1^{(\varrho)}, \ldots, \mathfrak{B}_h^{(\varrho)}\}$ Basissysteme h-ter Ordnung für $\mathfrak{Z}$ $(\varrho = 1, \ldots, r)$, so erhält man durch die Vereinigungsmenge $\bigcup_{\eta=1}^{h} \mathfrak{B}_\eta$ der kartesischen Produkte $\mathfrak{B}_\eta$ der Mengen $\mathfrak{B}_\eta^{(1)}, \ldots, \mathfrak{B}_\eta^{(r)}$ $(\eta = 1, \ldots, h)$ eine Basis h-ter Ordnung für $\mathfrak{Z}_r$.

---

[2]) Wenn $O \notin \mathfrak{M} \cap \left\{\bigcap_{\eta=1}^{h} \mathfrak{B}_\eta\right\}$ ist, braucht diese Behauptung nicht zu gelten, wie das Beispiel

$$\mathfrak{M} = \mathfrak{Z} - \{0, 1\} = \{2, 3, 4, \ldots\}$$

mit der Multiplikation als Komposition für $h \geqq 2$ zeigt. Denn Primzahlen lassen sich nicht als Produkt von Elementen aus Untermengen von $\mathfrak{M}$ darstellen.

[3]) Für die Definition der Anzahlfunktion siehe Nr. 6.

Beweis. Ist $\mathfrak{z} \in \mathfrak{Z}_r$, $\mathfrak{z} = \{z_1, \ldots, z_r\}$, dann können wir jedes z_ϱ darstellen als $z_\varrho = b_1^{(\varrho)} + \cdots + b_h^{(\varrho)} (\varrho = 1, \ldots, r)$ mit $b_\eta^{(\varrho)} \in \mathfrak{B}_\eta^{(\varrho)}$ und $\mathfrak{z}$ als

$$\mathfrak{z} = \{b_1^{(1)}, \ldots, b_1^{(r)}\} + \{b_2^{(1)}, \ldots, b_2^{(r)}\} + \cdots + \{b_h^{(1)}, \ldots, b_h^{(r)}\},$$

wobei $\{b_\eta^{(1)}, \ldots, b_\eta^{(r)}\} \in \mathfrak{B}_\eta$ ist.

5. Um in $\mathfrak{G}$ eine gewisse Halbordnung einzuführen, setzen wir voraus, daß es in $\mathfrak{G}$ eine Norm gibt, d. h. jedem $x \in \mathfrak{G}$ sei eindeutig eine reelle Zahl $\| x \|$ zugeordnet[4]) mit folgenden Eigenschaften:

(12) *Der Wertevorrat der Norm hat nur an seiner oberen Grenze einen Häufungspunkt, der auch ∞ sein darf.*

(13) *Es gibt zu jedem reellen ξ höchstens endlich viele Elemente $x_1, \ldots, x_n \in \mathfrak{G}$ mit $\| x_1 \| = \cdots = \| x_n \| = \xi$.*

(14) $\| O \| = 0$; $\| x \| \neq 0$, *wenn* $x \neq O$.

(15) $\| \sigma(x_1, \ldots, x_n) \| \geqq \| x_\nu \|$ $(\nu = 1, \ldots, n)$, *sofern* $\sigma(x_1, \ldots, x_n) \neq \omega$ *ist.*

Aus $\| x \| = \| \sigma(x, O \| \geqq \| O \|$ folgt $\| x \| > 0$ für $x \neq O$. Also ist die Norm eine reelle nichtnegative Funktion der Elemente $x \in \mathfrak{G}$. Die Forderungen (12) und (13) bewirken, daß die Menge $\mathfrak{G}$ abzählbar sein muß. Alle Aussagen, die beim Beweis (12) und (13) nicht benutzen, gelten somit auch für nicht abzählbare Mengen $\mathfrak{G}$.

Es genügt, wenn wir in (12) nur den Häufungspunkt ∞ zulassen. Denn ist in $\mathfrak{G}$ eine Norm $\| x \|$ $(x \in \mathfrak{G})$ mit den Bedingungen (12) bis (15) erklärt, wobei der Wertevorrat der Norm den (endlichen) Häufungspunkt $H > 0$ hat, dann definieren wir durch $((x)) = \dfrac{\| x \|}{H - \| x \|}$ eine neue Norm in $\mathfrak{G}$. Diese so erklärte Norm hat ∞ als einzigen Häufungspunkt und genügt den Bedingungen (12) bis (15). Beim Nachweis der Eigenschaft (15) geht man so vor: Zunächst zeigen wir, daß aus $\| x_1 \| \leqq \| x_2 \|$ folgt $((x_1)) \leqq ((x_2))$. Denn nach Voraussetzung wird $H - \| x_1 \| \geqq H - \| x_2 \|$, also

$$((x_1)) = \frac{\| x_1 \|}{H - \| x_1 \|} \leqq \frac{\| x_2 \|}{H - \| x_2 \|} = ((x_2)).$$

Daraus folgt aber Eigenschaft (15).

6. *Anzahlfunktion und Dichte.* Mit Hilfe der Norm definieren wir für eine Menge $\mathfrak{A} \subseteq \mathfrak{G}$ bzw. für ein System $A = \{\mathfrak{A}_1, \ldots, \mathfrak{A}_n\}$ von Mengen $\mathfrak{A}_\nu \subseteq \mathfrak{G}$ $(\nu = 1, \ldots, n;\ 1 \leqq n < \infty)$ eine Anzahlfunktion. Ist $\xi \geqq 0$ reell, so verstehen wir unter der Anzahlfunktion der Menge $\mathfrak{A}$ die Summe

$$\mathfrak{A}(\xi) = \sum_{\substack{a \in \mathfrak{A} \\ 0 < \| a \| \leq \xi}} 1 \quad \textit{und} \quad \mathfrak{A}(0) = 0.$$

Wegen der Voraussetzungen (12) und (13) über die Norm ist $\mathfrak{A}(\xi)$ für jedes reelle $\xi \geqq 0$ endlich[5]).

Die Anzahlfunktion des Systems A erklären wir durch

$$A(\xi) = \sum_{\nu=1}^{n} \mathfrak{A}_\nu(\xi).$$

Für die Anzahlfunktion der Vereinigungsmenge $\mathfrak{A} = \bigcup_{\nu=1}^{n} \mathfrak{A}_\nu$ haben wir dann, wie man leicht erkennt,

$$\frac{1}{n} A(\xi) \leqq \mathfrak{A}(\xi) \leqq A(\xi) = \sum_{\nu=1}^{n} \mathfrak{A}_\nu(\xi).$$

---

[4]) Es würde genügen, wenn $\| x \|$ einer geordneten Menge angehört.

[5]) Sonst bezeichnet man immer die Anzahlfunktion mit dem entsprechenden lateinischen Buchstaben. Diese wollen wir aber hier für Systeme von Mengen reservieren.

Ganz in Analogie zum bisherigen Gebrauch in der Literatur definieren wir

$$\operatorname*{fin}_{\substack{x \in \mathfrak{G} \\ x \neq O}} \frac{\mathfrak{A}(\|x\|)}{\mathfrak{G}(\|x\|)} = D(\mathfrak{A}) \text{ als Schnirelmannsche Dichte,}$$

$$\underline{\lim}_{\substack{x \in \mathfrak{G} \\ x \neq O}} \frac{\mathfrak{A}(\|x\|)}{\mathfrak{G}(\|x\|)} = \underline{D}(\mathfrak{A}) \text{ als (untere) asymptotische Dichte,}$$

$$\overline{\lim}_{\substack{x \in \mathfrak{G} \\ x \neq O}} \frac{\mathfrak{A}(\|x\|)}{\mathfrak{G}(\|x\|)} = \overline{D}(\mathfrak{A}) \text{ als obere asymptotische Dichte}$$

und, sofern vorhanden,

$$\lim_{\substack{x \in \mathfrak{G} \\ x \neq O}} \frac{\mathfrak{A}(\|x\|)}{\mathfrak{G}(\|x\|)} = D^*(\mathfrak{A}) \text{ als natürliche Dichte}$$

der Menge $\mathfrak{A}$.

§ 2. Einige allgemeine Sätze über Basissysteme und Basen.

7. Wir wollen in diesem Paragraphen einige Aussagen beweisen, die den Basisbegriff in der allgemeinen Form ohne zusätzliche Forderungen benutzen. Nur beim Beweis von Satz 2 wird Gebrauch von den Bedingungen (12) bis (15) gemacht, so daß alle anderen Aussagen auch für nichtabzählbare Mengen $\mathfrak{M}$ gelten.

Satz 1. *Seien* $\mathfrak{M}_i \leqq \mathfrak{G}$ *mit* $O \in \bigcap_{i=1}^{n} \mathfrak{M}_i$ *und* $\{\mathfrak{B}_1^{(i)}, \ldots, \mathfrak{B}_h^{(i)}\}$ *Basissysteme der Ordnung* $h (1 \leqq h \leqq \infty)$ *für* $\mathfrak{M}_i (i = 1, \ldots, n;\ 1 \leqq n \leqq \infty)$. *Dann ist* $\left\{ \bigcup_{i=1}^{n} \mathfrak{B}_1^{(i)}, \ldots, \bigcup_{i=1}^{n} \mathfrak{B}_h^{(i)} \right\}$ *Basissystem der Ordnung* h *für* $\bigcup_{i=1}^{n} \mathfrak{M}_i$.

Beweis. Ist $x \in \mathfrak{M}_i$, so hat x seine Darstellung $x = \sigma(b_1^{(i)}, \ldots, b_h^{(i)})$, $b_\eta^{(i)} \in \mathfrak{B}_\eta^{(i)} \leqq \bigcup_{i=1}^{n} \mathfrak{B}_\eta^{(i)}$. Weil diese Aussage für alle Mengen $\mathfrak{M}_i (i = 1, \ldots, n)$ gilt, ist Satz 1 bewiesen.

Bemerkungen: a) Eine entsprechende Aussage läßt sich für Basen h-ter Ordnung $(1 \leqq h \leqq \infty)$ zeigen.

b) Satz 1 gilt auch mit Zusatzbedingung (11).

Ist $\mathfrak{G}$ unendlich, so ist die Gesamtheit aller Basissysteme $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ der Ordnung $h (h \geqq 1)$ für $\mathfrak{M} \leqq \mathfrak{G}$ $(O \in \mathfrak{M})$ von der Mächtigkeit des Kontinuums. Dabei nennen wir zwei Systeme $\{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ und $\{\mathfrak{B}_1^*, \ldots, \mathfrak{B}_h^*\}$ genau dann gleich, wenn $\mathfrak{B}_\eta = \mathfrak{B}_\eta^*$ gilt $(\eta = 1, \ldots, h)$. Zum Beweis dieser Aussage braucht man nur $\mathfrak{B}_1 = \mathfrak{M}$ und für $\mathfrak{B}_2 = \cdots = \mathfrak{B}_h$ irgendeine Untermenge von $\mathfrak{G}$, die das Element O enthält, zu nehmen.

Für Basen kann jedoch der Fall eintreten, daß eine Menge $\mathfrak{M}$ nur *eine* Basis $\mathfrak{B}$ der Ordnung h besitzt. Dann gilt für jedes $x \in \mathfrak{M}$

$$x \notin h(\mathfrak{M} - \{x\}) \tag{16}$$

und umgekehrt.

Beweis. Weil $\mathfrak{M}$ nur eine Basis $\mathfrak{B}$ der Ordnung h besitzen soll, gilt $\mathfrak{B} = \mathfrak{M}$. Dann hat aber jedes $x \in \mathfrak{M}$ als einzige Darstellungen

$$x = \sigma(x, O, \ldots, O) = \sigma(O, \ldots, O, x, O, \ldots, O) = \sigma(O, \ldots, O, x).$$

Wenn umgekehrt für jedes Element $x \in \mathfrak{M}$ gilt $x \notin h(\mathfrak{M} - \{x\})$, dann ist $\mathfrak{B} = \mathfrak{M}$ die einzige Basis der Ordnung h für $\mathfrak{M}$.

Bemerkung: Bedingung (16) läßt sich auch so ausdrücken, daß jedes Element zu seiner eigenen Darstellung benötigt wird.

Allgemeiner wollen wir zeigen

Satz 2. *Sei $\mathfrak{M} \leqq \mathfrak{G}$ mit $O \in \mathfrak{M}$. Dann ist die Klasse K der Basen $\mathfrak{B}$ der Ordnung h für $\mathfrak{M}$ entweder endlich oder von der Mächtigkeit des Kontinuums*[6]).

Beweis. Wir betrachten zunächst $h < \infty$ und unterscheiden zwei Fälle:

1.) Es gibt eine Basis $\mathfrak{B}$ der Ordnung h für $\mathfrak{M}$ derart, daß $\mathfrak{G} - \mathfrak{B}$ eine unendliche Menge ist. Dann ist die Klasse K von der Mächtigkeit des Kontinuums.

2.) Für jede Basis $\mathfrak{B}$ der Ordnung h für $\mathfrak{M}$ ist $\mathfrak{G} - \mathfrak{B}$ endlich. Dann ist auch $\mathfrak{G} - \mathfrak{M}$ endlich (oder leer). Wir wollen zeigen, daß in diesem Fall die Klasse K endlich ist. Angenommen, K wäre unendlich. Dann gibt es unendlich viele verschiedene Untermengen $\mathfrak{X}_\nu = \{\xi_1^{(\nu)}, \ldots, \xi_{k_\nu}^{(\nu)}\}$ mit $\| \xi_\varkappa^{(\nu)} \| \leqq \| \xi_{\varkappa+1}^{(\nu)} \|$ von $\mathfrak{G}$, so daß $\mathfrak{B}_\nu = \mathfrak{G} - \mathfrak{X}_\nu$ Basis der Ordnung h für $\mathfrak{M}$ ist und alle Elemente $x \in \mathfrak{M}$ mit $\| x \| > \| \xi_{k_\nu}^{(\nu)} \|$, die dann in $\mathfrak{B}_\nu$ enthalten sind, wegen (15) zu ihrer eigenen Darstellung benötigt werden. Aus der Klasse dieser Mengen $\mathfrak{X}_\nu$ bestimmen wir $h+1$ Mengen $\mathfrak{X}_1, \ldots, \mathfrak{X}_{h+1}$ mit den Eigenschaften

$$0 < \| \xi_1^{(1)} \| \leqq \| \xi_{k_1}^{(1)} \| < \| \xi_1^{(2)} \| \leqq \| \xi_{k_2}^{(2)} \| < \cdots < \| \xi_1^{(h+1)} \| \leqq \| \xi_{k_{h+1}}^{(h+1)} \|.$$

Eine solche Auswahl ist möglich: Seien schon t Mengen $\mathfrak{X}_1, \ldots, \mathfrak{X}_t$, $1 \leqq t \leqq h$, mit den geforderten Eigenschaften bestimmt. Dann gibt es wegen (12) und (13) eine Menge $\mathfrak{X}_r$ mit $\| \xi_{k_r}^{(r)} \| > \| \xi_{k_t}^{(t)} \|$. Aus $\mathfrak{X}_r$ bilden wir $\widetilde{\mathfrak{X}}_r$, indem wir setzen

$$\widetilde{\mathfrak{X}}_r = \mathfrak{X}_r \cap \{x \in \mathfrak{G};\ \| x \| > \| \xi_{k_t}^{(t)} \|\}.$$

Aus $\widetilde{\mathfrak{X}}_r$ konstruieren wir schließlich $\mathfrak{X}_{t+1}$, indem wir $\widetilde{\mathfrak{X}}_r$ um endlich viele Elemente mit Norm $\geqq \| \xi_{k_r}^{(r)} \|$ aus $\mathfrak{G}$ vermehren, so daß $\mathfrak{G} - \mathfrak{X}_{t+1}$ Basis der Ordnung h für $\mathfrak{M}$ ist und alle Elemente aus $\mathfrak{G} - \mathfrak{X}_{t+1}$ mit Norm $> \| \xi_{k_{t+1}}^{(t+1)} \| = \max\limits_{x \in \mathfrak{X}_{t+1}} \| x \|$ zu ihrer eigenen Darstellung benötigt werden.

Sei weiterhin $\| \xi_{k_\nu}^{(\nu)} \| > \| \xi_{k_{h+1}}^{(h+1)} \|$ und $\xi_{k_\nu}^{(\nu)} \in (\mathfrak{M} \cap \mathfrak{X}_\nu)$. Dann ist auf Grund der Konstruktion der Mengen $\mathfrak{X}_1, \ldots, \mathfrak{X}_{h+1}$ das Element $\xi_{k_\nu}^{(\nu)}$ als Summe von h Elementen aus $\mathfrak{B}_\nu = \mathfrak{G} - \mathfrak{X}_\nu$ nur mit Hilfe von Elementen aus jeder Menge $\mathfrak{X}_t$, $1 \leqq t \leqq h+1$, darstellbar, was einen Widerspruch bedeutet.

Ist $\mathfrak{B}$ eine Basis unendlicher Ordnung für $\mathfrak{M}$, so muß natürlich $\mathfrak{G} - \mathfrak{B}$ eine unendliche Menge sein. Also ist für $h = \infty$ die Klasse K von der Mächtigkeit des Kontinuums.

Zusatz. Es gibt höchstens $h+1$ Basen $\mathfrak{B}_1, \ldots, \mathfrak{B}_{h+1}$ bei denen

$$\{\mathfrak{G} - \mathfrak{B}_i\} \cap \bigcup_{\substack{\eta=1 \\ \eta \neq i}}^{h+1} \{\mathfrak{G} - \mathfrak{B}_\eta\}$$

leer ist ($i = 1, \ldots, h+1$) und jedes Element aus

$$\mathfrak{B}_\eta \cap \{x \in \mathfrak{G};\ \| x \| > \max \| y \|;\ y \in \mathfrak{G} - \mathfrak{B}_\eta\}$$

zu seiner eigenen Darstellung benötigt wird. Die Begründung zu dieser Aussage ist im Beweis zu Satz 2 enthalten.

§ 3. Minimalsysteme und Minimalbasen.

8. Dem Basisbegriff sollen nun gewisse Zusatzbedingungen auferlegt werden, die bewirken, daß wir Basen mit irgendwie „möglichst wenig Elementen" erhalten. Zur Präzisierung dieser Minimalforderung werden im folgenden einige Möglichkeiten aufgezeigt (vgl. Stöhr [15]).

---

[6]) Satz 2 läßt sich mit einigen Zusatzüberlegungen auch ohne Benutzung der Bedingung (15) beweisen.

Definition 5. *Sei $\mathfrak{M} \leqq \mathfrak{G}$ mit $O \in \mathfrak{M}$. Ein Basissystem $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ der Ordnung $h (1 \leqq h \leqq \infty)$ für $\mathfrak{M}$ heißt Minimalsystem, wenn kein echtes Untersystem B^* von B Basissystem der Ordnung h für $\mathfrak{M}$ ist.*

Dabei verstehen wir unter einem Untersystem von $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ ein System $B^* = \{\mathfrak{B}_1^*, \ldots, \mathfrak{B}_h^*\}$ mit $\mathfrak{B}_\eta^* \leqq \mathfrak{B}_\eta$ $(\eta = 1, \ldots, h)$ und schreiben $B^* \leqq B$. Gilt für einen Index η hierbei $\mathfrak{B}_\eta^* < \mathfrak{B}_\eta$, so sprechen wir von einem echten Untersystem und kennzeichnen diesen Sachverhalt durch $B^* < B$.

Im Sonderfall $\mathfrak{B}_1 = \cdots = \mathfrak{B}_h$ erhalten wir aus Definition 5

Definition 6. *Eine Basis $\mathfrak{B}$ der Ordnung h $(1 \leqq h \leqq \infty)$ für $\mathfrak{M}$ heißt Minimalbasis, wenn keine echte Teilmenge $\mathfrak{B}^*$ von $\mathfrak{B}$ Basis der Ordnung h für $\mathfrak{M}$ ist, d. h. jedes Element $b \in \mathfrak{B}$ zur Darstellung eines Elements $x \in \mathfrak{M}$ benötigt wird.*

Wir können somit schreiben

$$h\mathfrak{B} \geqq \mathfrak{M}, \quad \text{aber } h(\mathfrak{B} - \{b\}) \not\geqq \mathfrak{M}$$

für jedes $b \in \mathfrak{B}$.

Die Existenz von Minimalsystemen zeigt folgender

Satz 3. *In jedem Basissystem $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ der Ordnung h $(1 \leqq h \leqq \infty)$ für $\mathfrak{M}$ ist ein Minimalsystem der Ordnung h für $\mathfrak{M}$ als (echtes oder unechtes) Untersystem enthalten.*

Beweis. Wir bilden eine (endliche oder unendliche) Folge $B = B_0 > \cdots > B_n > \cdots$ von induktiv auseinander hervorgehenden Basissystemen der Ordnung h für $\mathfrak{M}$, wobei wir $B_0 = B$ setzen. Sei $B_n (n \geqq 0)$ schon konstruiert. Entweder ist $B_n = \{\mathfrak{B}_1^{(n)}, \ldots, \mathfrak{B}_h^{(n)}\}$ Minimalsystem der Ordnung h für $\mathfrak{M}$, dann brechen wir die Folge mit B_n ab, oder es gibt ein Element b^* in einer Menge $\mathfrak{B}_i^{(n)}$, so daß auch

$$(17) \quad B_n^* = \{\mathfrak{B}_1^{*(n)}, \ldots, \mathfrak{B}_h^{*(n)}\} \text{ mit } \mathfrak{B}_\eta^{*(n)} = \mathfrak{B}_\eta^{(n)} \quad (\eta = 1, \ldots, h;\ \eta \neq i)$$
$$\text{und } \mathfrak{B}_i^{*(n)} = \mathfrak{B}_i^{(n)} - \{b^*\}$$

Basissystem der Ordnung h für $\mathfrak{M}$ ist. Sei b in $\mathfrak{B}_i^{(n)}$ so beschaffen, daß für kein Element mit kleinerer Norm aus $\bigcup_{\eta=1}^{h} \mathfrak{B}_\eta^{(n)}$ die Eigenschaft (17) zutrifft. Dann setzen wir $B_{n+1} = \{\mathfrak{B}_1^{(n+1)}, \ldots, \mathfrak{B}_h^{(n+1)}\}$ mit $\mathfrak{B}_\eta^{(n+1)} = \mathfrak{B}_\eta^{(n)}$ $(\eta = 1, \ldots, h;\ \eta \neq i)$ und $\mathfrak{B}_i^{(n+1)} = \mathfrak{B}_i^{(n)} - \{b\}$. Das System $\widetilde{B} = \left\{ \bigcap_{n=0}^{\infty} \mathfrak{B}_1^{(n)}, \ldots, \bigcap_{n=0}^{\infty} \mathfrak{B}_h^{(n)} \right\}$ ist dann Minimalsystem der Ordnung h für $\mathfrak{M}$ mit $\widetilde{B} \leqq B$.

Für $\mathfrak{B}_1 = \cdots = \mathfrak{B}_h = \mathfrak{B}$ geht Satz 3 über in

Satz 4. *In jeder Basis $\mathfrak{B}$ der Ordnung h $(1 \leqq h \leqq \infty)$ für $\mathfrak{M}$ ist eine Minimalbasis der Ordnung h für $\mathfrak{M}$ als (echte oder unechte) Teilmenge enthalten.*

Bemerkungen: a) Die Sätze 3 und 4 gelten auch mit Zusatzbedingung (11). b) Besitzt eine Menge $\mathfrak{M}$ Basen genau h-ter Ordnung, dann gibt es auch Minimalbasen genau h-ter Ordnung für $\mathfrak{M}$.

9. Für die Menge der nichtnegativen ganzen Zahlen weiß man, daß die Klasse der so definierten Minimalbasen von der Mächtigkeit des Kontinuums ist. Die Übertragung dieses Ergebnisses gibt der folgende

Satz 5. *Sei $\mathfrak{M} \leqq \mathfrak{G}$, $O \in \mathfrak{M}$ und $\mathfrak{M}$ unendlich. Alle $x \in \mathfrak{M}$ mit $\| x \| \geqq \xi$ seien darstellbar als $x = \sigma(a_1, \ldots, a_h)$ $(a_\eta \in \mathfrak{G})$ mit $\| x \| > \| a_\eta \| \geqq \varphi(\| x \|)$ oder $a_\eta = 0$, wobei $\varphi(t)$ eine monoton wachsende nicht beschränkte reelle Funktion bedeutet. Dann ist die Klasse der Minimalbasen der Ordnung h $(2 \leqq h < \infty)$ für $\mathfrak{M}$ kontinuummächtig* [7]).

[7]) Satz 5 gilt auch, wenn $\mathfrak{G}$ die Menge der nichtnegativen rationalen Zahlen ist.

Beweis. Sei $0 = \xi_0 < \xi_1 < \xi_2 < \cdots < \xi_n < \cdots$ die Folge der verschiedenen Werte der Norm, die entsteht, wenn x alle Elemente aus $\mathfrak{M}$ durchläuft. (Wir nehmen o. B. d. A. an, daß der Wertevorrat der Norm keinen endlichen Häufungspunkt hat.) Sei $\mathfrak{B}_N$ Minimalbasis der Ordnung h für $\{x \in \mathfrak{M};\ \| x \| \leqq \xi_N\}$ mit $\xi_N \geqq \xi$, die sich nach Satz 4 konstruieren läßt.

Nun wenden wir eine induktive Konstruktionsmethode an. Sei $\mathfrak{B}_n$ als Minimalbasis der Ordnung h für $\{x \in \mathfrak{M};\ \| x \| \leqq \xi_n\}$, $n \geqq N$, schon konstruiert. Wir setzen $\mathfrak{B}_{n+1} = \mathfrak{B}_n$, wenn $h\mathfrak{B}_n \geqq \{x \in \mathfrak{M};\ \| x \| \leqq \xi_{n+1}\}$ ist. Für $h\mathfrak{B}_n \ngeqq \{x \in \mathfrak{M};\ \| x \| \leqq \xi_{n+1}\}$ bilden wir $\mathfrak{B}^*_{n+1}$ durch $\mathfrak{B}^*_{n+1} = \mathfrak{B}_n \cup \mathfrak{A}_{n+1}$ mit

(i) $\mathfrak{A}_{n+1} = \{x \in \mathfrak{M};\ \| x \| = \xi_{n+1}\}$ oder

(ii) $\mathfrak{A}_{n+1} \leqq \{x \in \mathfrak{G};\ \xi_{n+1} > \| x \| \geqq \varphi(\xi_{n+1})\}$,

so daß $h(\mathfrak{A}_{n+1} \cup \{O\}) \geqq \{x \in \mathfrak{M};\ \| x \| = \xi_{n+1}\}$ ist. Diese letztere Induktionsmöglichkeit (ii) ist aber nur erlaubt, wenn $\varphi(\xi_{n+1}) > \xi_{n'}$ bzw. $> \xi_N$ ist, wobei n' den Induktionsschritt bedeutet, bei dem zum letztenmal (ii) angewandt wurde.

Nun bilden wir aus $\mathfrak{B}^*_{n+1}$ eine Minimalbasis $\mathfrak{B}_{n+1}$ der Ordnung h für

$$\{x \in \mathfrak{M};\ \| x \| \leqq \xi_{n+1}\}$$

nach Satz 4.

Durch die Vereinigungsmenge jeder solchen Folge von induktiv auseinander hervorgehenden (endlichen) Mengen $\mathfrak{B}_n$, also durch

$$\bigcup_{\substack{n=N \\ \mathfrak{B}_N \leqq \cdots \leqq \mathfrak{B}_n \leqq \mathfrak{B}_{n+1} \leqq \cdots}}^{\infty} \mathfrak{B}_n = \mathfrak{B},$$

erhalten wir eine Minimalbasis der Ordnung h für $\mathfrak{M}$. Jeder solchen Basis ordnen wir entsprechend wie in [6], Satz 12, umkehrbar eindeutig den Weg eines unendlichen Graphen zu. Jeder Weg hat unendlich viele Verzweigungspunkte, da unendlich oft die Wahl zwischen den beiden Induktionsmöglichkeiten (i) und (ii) besteht. Demnach hat die Menge der Wege die Mächtigkeit des Kontinuums und somit auch die Klasse der so konstruierten Minimalbasen der Ordnung h für $\mathfrak{M}$.

Bemerkung zu Satz 5. Für $h = \infty$ braucht dieser Satz nicht zu gelten. Nehmen wir beispielsweise $\mathfrak{G} = \mathfrak{M} = \mathfrak{Z} = \{0, 1, 2, \ldots\}$ und die gewöhnliche Addition als Komposition. Dann ist $\mathfrak{B} = \{0, 1\}$ die einzige Minimalbasis unendlicher Ordnung für $\mathfrak{Z}$. Ein anderes Beispiel liefert die Menge $\mathfrak{G} = \mathfrak{Z} - \{0\}$ mit der Multiplikation als Komposition, für die die Menge der Primzahlen einschließlich 1 die einzige Minimalbasis unendlicher Ordnung ist.

Andere Beispiele zeigen, daß die Voraussetzung von Satz 5 keine notwendige Bedingung ist. Es genügt dabei die Forderung über die Darstellbarkeit für eine geeignete unendliche Folge von Elementen $x \in \mathfrak{M}$. Betrachten wir beispielsweise $\mathfrak{G} = \mathfrak{Z} - \{0, 1\}$ und nehmen der Einfachheit halber $h = 2$. Sei weiter $\mathfrak{B} = \{b_0, b_1, \ldots, b_k, \ldots\}$ eine beliebige Minimalbasis 2-ter Ordnung für $\mathfrak{Z}$ (mit der Addition als Komposition). Dann bildet die Menge $\mathfrak{C}^*$, die aus allen Produkten $p_1 p_2 \cdots p_{b_k}$ besteht, wobei die p_i (nicht notwendig verschiedene) Primzahlen sind und b_k alle positiven Elemente aus $\mathfrak{B}$ durchläuft, eine Basis 2. Ordnung für $\mathfrak{G}$ mit der Multiplikation als Komposition. Aus $\mathfrak{C}^*$ bilden wir nach Satz 4 eine Minimalbasis 2. Ordnung $\mathfrak{C}$ für $\mathfrak{G}$; dabei erhalten wir aus verschiedenen Mengen $\mathfrak{B}$ verschiedenen Basen $\mathfrak{C}^*$ und dann auch verschiedene Minimalbasen $\mathfrak{C}$.

Das Analogon zu Satz 5 für Basissysteme wird durch folgenden Satz dargestellt:

Satz 6. *Sei $\mathfrak{M} \leqq \mathfrak{G}$, $O \in \mathfrak{M}$ und $\mathfrak{M}$ unendlich und es gelte die Voraussetzung von Satz 5. Dann ist die Klasse der Minimalsysteme der Ordnung h $(2 \leqq h < \infty)$ für $\mathfrak{M}$ kontinuummächtig.*

Beweis. Sei $\mathfrak{B}$ Minimalbasis der Ordnung h für $\mathfrak{M}$. Durch das System $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ mit $\mathfrak{B}_1 = \cdots = \mathfrak{B}_h = \mathfrak{B}$ erhalten wir ein Basissystem der Ordnung h für $\mathfrak{M}$. Aus diesem konstruieren wir auf Grund von Satz 3 ein Minimalsystem der Ordnung h für $\mathfrak{M}$. Da verschiedene Minimalbasen $\mathfrak{B}$ zu verschiedenen Minimalsystemen führen, folgt unter Benutzung von Satz 5 die Behauptung.

Bei der Übertragung weiterer Sätze über Basen muß man an die Menge $\mathfrak{G}$ noch mehr Forderungen stellen, wie die folgenden Beispiele zeigen:

Satz 7. *Sei $\mathfrak{M} \leqq \mathfrak{G}$, $O \in \mathfrak{M}$ und $\mathfrak{M}$ unendlich; sei ferner $\mathfrak{A} < \mathfrak{G}$ endlich. Seien schließlich die folgenden Voraussetzungen erfüllt:*

(A) *zu jedem $a \in \mathfrak{G}$ und jedem $x \in \mathfrak{M}$ mit $\| x \| \geqq \xi$ gibt es eine eindeutige Lösung $\zeta \in \mathfrak{G}$ von $x = \sigma(a, \zeta)$;*

(B) *$\mathfrak{G}$ ist kommutativ;*

(C) *$\mathfrak{G}$ ist assoziativ;*

(D) *in $\mathfrak{G}$ gilt $\| \sigma(x_1, x_2) \| > \| x_1 \|$ für $\| x_2 \| > 0$ $(x_\nu \in \mathfrak{G})$.*

Dann gibt es Minimalbasen $\mathfrak{B}$ der Ordnung $h (2 \leqq h < \infty)$ für $\mathfrak{M}$ mit $\mathfrak{A} < \mathfrak{B}$.

Beweis. Sei $\mathfrak{A} = \{a_1, \ldots, a_r\}$, wobei wir uns o. B. d. A. auf $O \in \mathfrak{A}$ beschränken können. Weiter sei $0 = \xi_0 < \xi_1 < \cdots < \xi_n < \cdots$ die Folge der verschiedenen Werte der Norm, die entsteht, wenn x alle Elemente aus $\mathfrak{M}$ durchläuft.

I. Wir behandeln zuerst den Fall $h = 2$. Dann gilt für ein geeignetes Element $x_{n_0} \in \mathfrak{M}$

$$\max_{\varrho = 1, \ldots, r} (\| a_\varrho \|, \xi) \leqq \| x_{n_0} \| = \xi_N .$$

Hiermit setzen wir $\mathfrak{A}_0 = (\mathfrak{A} \cup \mathfrak{M}) \cap \{x \in \mathfrak{G};\ 0 < \| x \| \leqq \xi_N\} = \{a'_1, \ldots, a'_s\}$ und $\mathfrak{B}_N = \mathfrak{A}_0 \cup \{O\}$. Ist für ein $n \geqq N$ eine Menge $\mathfrak{B}_n$ schon konstruiert, so setzen wir

(i) wenn für alle $x \in \mathfrak{M}$ mit $\| x \| \leqq \xi_{n+1}$ gilt $x \in 2\mathfrak{B}_n$, die neue Menge $\mathfrak{B}_{n+1} = \mathfrak{B}_n$,

(ii) wenn genau für $\{x^{(1)}, \ldots, x^{(t)}\} < \mathfrak{M}$ mit $\| x^{(\tau)} \| = \xi_{n+1}$ gilt $x^{(\tau)} \notin 2\mathfrak{B}_n$ $(\tau = 1, \ldots, t)$ eine neue Menge $\mathfrak{B}^*_{n+1}$ an als

$$\mathfrak{B}^*_{n+1} = \mathfrak{B}^*_n \cup \mathfrak{A}^*_{n+1},$$

wobei $\mathfrak{A}^*_{n+1}$ und $\mathfrak{B}^*_n$ folgendermaßen bestimmt sind: Sei

(α) $\mathfrak{A}_{n+1} = \{x^{(1)}, \ldots, x^{(t)}\}$ bzw.

(β) $\mathfrak{A}_{n+1} = \{\zeta^{(1)}, x^{(2)}, \ldots, x^{(t)}\}$ und $\zeta^{(1)} \in \mathfrak{G}$ die Lösung von

$$x^{(1)} = \sigma(a'_\nu, \zeta^{(1)}) \qquad (\nu \in \{1, \ldots, s\}).$$

Der Fall (β) tritt immer dann ein, wenn $\| \zeta^{(1)} \| > \xi_{n'}$ (bzw. $> \xi_N$) ist, was wegen (12) und (13) sicher einmal eintritt, wobei n' den Induktionsschritt bedeutet, bei dem zum letzten Mal Konstruktion (β) angewandt wurde.

Dann bestimmen wir eine Minimalbasis 2-ter Ordnung $\mathfrak{B}^*_{n+1} \leqq \mathfrak{B}_n \cup \mathfrak{A}_{n+1}$ für $\{x \in \mathfrak{M};\ \| x \| \leqq \xi_{n+1}\}$, d. h. es wird $\mathfrak{B}^*_{n+1} = \mathfrak{B}^*_n \cup \mathfrak{A}^*_{n+1}$ mit $\mathfrak{B}^*_n \leqq \mathfrak{B}_n$ und $\mathfrak{A}^*_{n+1} \leqq \mathfrak{A}_{n+1}$. Offenbar wird $\mathfrak{A}^*_{n+1}$ nicht leer und wir setzen $\mathfrak{B}_{n+1} = \mathfrak{B}^*_{n+1} \cup \mathfrak{A}_0$.

Nun soll a'_ν bei den Induktionsschritten der Form (ii) (β) alle Elemente von $\mathfrak{A}_0$ durchlaufen, was nach endlich vielen Schritten der Fall ist; von da an folgen die Induktionsschritte allein nach der Form (i) bzw. (ii) (α).

Die Vereinigungsmenge $\mathfrak{B} = \bigcup_{n=N}^{\infty} \mathfrak{B}_n$ erfüllt dann folgende Eigenschaften mit $h = 2$: Die Menge $\mathfrak{B}$ ist

1. Basis der Ordnung h für $\mathfrak{M}$ (nach Konstruktion),

2. Obermenge von $\mathfrak{A}_0$ (nach Konstruktion),

3. Minimalbasis der Ordnung h für $\mathfrak{M}$ nach Konstruktion bzw. da auf Grund der Voraussetzungen (A), (B) und (D) das Element $x^{(1)}$ nur darstellbar ist als $x^{(1)} = \sigma(a'_\nu, \zeta^{(1)})$ bzw. als $x^{(1)} = \sigma(\zeta^{(1)}, a'_\nu)$. Denn wäre auch $\sigma(u, v) = \sigma(a'_\nu, \zeta^{(1)}) = x^{(1)}$, dann müßte u oder $v = \zeta^{(1)} \in \mathfrak{A}^*_{n+1}$ sein, was aber in jedem Fall zu einem Widerspruch führt.

II. Sei schon gezeigt, daß es für eine Ordnung h ($h \geqq 2$) eine Basis $\widetilde{\mathfrak{B}}$ für $\mathfrak{M}$ gibt, die die Eigenschaften 1. bis 3. erfüllt. Es gibt also zu jedem Element $a'_\nu \in \mathfrak{A}_0$ ein Element $x(a'_\nu) \in \mathfrak{M}$, das in der Form $x(a'_\nu) = \sigma(b_1, \ldots, b_h)$ ($b_\eta \in \widetilde{\mathfrak{B}}$) nicht ohne Benutzung des Elements a'_ν darstellbar ist; es gilt also $x(a'_\nu) \notin h(\widetilde{\mathfrak{B}} - \{a'_\nu\})$. Wir setzen $\max\limits_{\nu=1,\ldots,s} (\| x(a'_\nu) \|, \xi) = \xi_M$ und $\{x(a'_1), \ldots, x(a'_s)\} = \mathfrak{N}$. Dann ist die Menge $\mathfrak{C}'_0$ der Elemente $b \in \widetilde{\mathfrak{B}}$ mit $\| b \| \leqq \xi_M$ Basis der Ordnung h für $\mathfrak{M} \cap \{x \in \mathfrak{G};\ \| x \| \leqq \xi_M\}$. Aus $\mathfrak{C}'_0$ wählen wir jetzt eine Teilmenge $\mathfrak{C}_0$ derart aus, daß $(h+1)\,\mathfrak{C}_0 \geqq \mathfrak{M} \cap \{x \in \mathfrak{G};\ \| x \| \leqq \xi_M\}$ und $h\mathfrak{C}_0 \geqq \mathfrak{N}$ ist und keine echte Untermenge von $\mathfrak{C}_0$ diese Eigenschaften besitzt. Ersichtlicherweise gilt dabei $\mathfrak{A}_0 < \mathfrak{C}_0$.

Nun verwenden wir wieder eine induktive Konstruktionsmethode. Wir setzen dazu $\mathfrak{C}_0 = \mathfrak{B}_M$. Ist für ein $n \geqq M$ eine Menge $\mathfrak{B}_n$ schon konstruiert, so setzen wir

(i) wenn für alle $x \in \mathfrak{M}$ mit $\| x \| \leqq \xi_{n+1}$ gilt $x \in (h+1)\,\mathfrak{B}_n$, die neue Menge $\mathfrak{B}_{n+1} = \mathfrak{B}_n$,

(ii) wenn genau für $\{x^{(1)}, \ldots, x^{(t)}\} \in \mathfrak{M}$ mit $\| x^{(\tau)} \| = \xi_{n+1}$ gilt $x^{(\tau)} \notin (h+1)\,\mathfrak{B}_n$ ($\tau = 1, \ldots, t$), eine neue Menge $\mathfrak{B}^*_{n+1}$ an als $\mathfrak{B}^*_{n+1} = \mathfrak{B}^*_n \cup \mathfrak{A}^*_{n+1}$, wobei $\mathfrak{A}^*_{n+1}$ und $\mathfrak{B}^*_n$ folgendermaßen bestimmt sind: Sei

(α) $\mathfrak{A}_{n+1} = \{x^{(1)}, \ldots, x^{(t)}\}$ bzw.

(β) $\mathfrak{A}_{n+1} = \{\zeta^{(1)}, x^{(2)}, \ldots, x^{(t)}\}$, wobei $\zeta^{(1)} \in \mathfrak{G}$ die Lösung von $x^{(1)} = \sigma(x(a'_\nu), \zeta^{(1)})$ ist ($\nu \in \{1, \ldots, s\}$).

Der Fall (β) tritt immer dann ein, wenn $\| \zeta^{(1)} \| > \xi_n$, (bzw. $> \xi_M$) ist, wobei n' den Induktionsschritt bedeutet, bei dem zum letzten Mal Konstruktion (β) angewandt wurde.

Dann bestimmen wir eine Minimalbasis $(h+1)$-ter Ordnung $\mathfrak{B}^*_{n+1} \leqq \mathfrak{B}_n \cup \mathfrak{A}^*_{n+1}$ für $\{x \in \mathfrak{M};\ \| x \| \leqq \xi_{n+1}\}$, d. h. es wird $\mathfrak{B}^*_{n+1} = \mathfrak{B}^*_n \cup \mathfrak{A}^*_{n+1}$ mit $\mathfrak{B}^*_n \leqq \mathfrak{B}_n$ und $\mathfrak{A}^*_{n+1} \leqq \mathfrak{A}_{n+1}$. Offenbar wird $\mathfrak{A}^*_{n+1}$ nicht leer und wir setzen $\mathfrak{B}_{n+1} = \mathfrak{B}^*_{n+1} \cup \mathfrak{C}_0$.

Nun soll a'_ν bei den Induktionsschritten der Form (ii) (β) alle Elemente von $\mathfrak{C}_0$ durchlaufen, was nach endlich vielen Schritten der Fall ist; von da an folgen die Induktionsschritte allein nach der Form (i) bzw. (ii) (α).

Die Vereinigungsmenge $\mathfrak{B} = \bigcup_{n=M}^{\infty} \mathfrak{B}_n$ erfüllt dann die Eigenschaften 1. bis 3. für die Ordnung $h+1$, wie man auf Grund der Konstruktion erkennt und da $x^{(1)}$ — bis auf triviale Abänderungen — nur darstellbar ist als $x^{(1)} = \sigma(x(a'_\nu), \zeta^{(1)}) = \sigma(b_1, \ldots, h_h, \zeta^{(1)})$, wenn $x(a'_\nu) = \sigma(b_1, \ldots, b_h)$ ist.

Die entsprechende Aussage für Basissysteme gibt

Satz 8. *Sei $\mathfrak{M} \leqq \mathfrak{G}$, $O \in \mathfrak{M}$ und $\mathfrak{M}$ unendlich; seien ferner $\mathfrak{A}_\eta$ endliche Untermengen von $\mathfrak{G}$ $(\eta = 1, \ldots, h)$ und $\bigcap_{\eta=1}^{h} \mathfrak{A}_\eta = \{O\}$ oder leer. Gelten für $\mathfrak{G}$ die Voraussetzungen* (A) *bis* (D) *von Satz* 7, *dann gibt es ein Minimalsystem $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ h-ter Ordnung $(2 \leqq h < \infty)$ für $\mathfrak{M}$ mit $\mathfrak{A}_\eta \leqq \mathfrak{B}_\eta$ $(\eta = 1, \ldots, h)$.*

Beweis. Sei $\mathfrak{A} = \bigcup_{\eta=1}^{h} \mathfrak{A}_\eta$. Nach Satz 7 gibt es eine Minimalbasis $\mathfrak{B}$ der Ordnung h für $\mathfrak{M}$ mit $\mathfrak{A} < \mathfrak{B}$. Daher ist $\tilde{B} = \{\tilde{\mathfrak{B}}_1, \ldots, \tilde{\mathfrak{B}}_h\}$ mit $\tilde{\mathfrak{B}}_1 = \cdots = \tilde{\mathfrak{B}}_h = \mathfrak{B}$ Basissystem der Ordnung h für $\mathfrak{M}$. Aus $\tilde{B}$ konstruieren wir ein Minimalsystem h-ter Ordnung B für $\mathfrak{M}$, indem wir nach Satz 3 ein Untersystem von $\tilde{B}$ bilden, hierbei aber Elemente, die zu $\mathfrak{A}_i$ gehören, nur aus Mengen $\mathfrak{B}_\eta$, $\eta \neq i$, wegnehmen. Hierdurch erhalten wir ein Minimalsystem $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ der Ordnung h für $\mathfrak{M}$ mit den Eigenschaften $\mathfrak{A}_\eta \leqq \mathfrak{B}_\eta$ $(\eta = 1, \ldots, h)$.

In diesen Fragenkreis gehört auch der folgende

Satz 9. *Sei $\mathfrak{B}$ Basis der Ordnung h für $\mathfrak{M} \leqq \mathfrak{G}$, $O \in \mathfrak{M}$ und $\mathfrak{M}$ unendlich sowie $\mathfrak{G}$ assoziativ. In $\mathfrak{B}$ gibt es ein Element e, so daß jedes $x \in \mathfrak{M}$ bis auf endlich viele Ausnahmen als $x = \sigma(e, \ldots, e)$ darstellbar ist. Sei $\varphi(x)$ die kleinstmögliche Anzahl der Elemente bei der Darstellung $x = \sigma(e, \ldots, e)$ von x*[8]*. Dann läßt sich $\mathfrak{B}$ bis auf endlich viele Elemente als Vereinigungsmenge von Minimalbasen für $\mathfrak{M}$ darstellen.*

Beweis. Wir werden zeigen, daß es für fast alle $a \in \mathfrak{B}$ eine Minimalbasis $\mathfrak{B}^*$ einer Ordnung h^* für $\mathfrak{M}$ gibt mit $\mathfrak{B}^* \leqq \mathfrak{B}$ und $a \in \mathfrak{B}^*$. Damit ist aber die Behauptung bewiesen.

Die Menge $\tilde{\mathfrak{B}} = \{O, e, a\} \cup \{b \in \mathfrak{B};\ \varphi(b) > \varphi(x)\}$, wobei wir $x \in \mathfrak{M}$ bei genügend großem $\| a \|$ so wählen, daß

$$\left(\left[\frac{\varphi(x)}{\varphi(a)}\right] + \varphi(a) - 1\right) h < \varphi(x) \tag{18}$$

ist, ist Basis einer Ordnung $\tilde{h} \leqq \left(\left[\frac{\varphi(x)}{\varphi(a)}\right] + \varphi(a) - 1\right) h$ für $\mathfrak{M}$. Zunächst ist eine solche Wahl für x möglich, denn $\varphi(x)$ bleibt nicht beschränkt. Die Basiseigenschaft von $\tilde{\mathfrak{B}}$ folgt daraus, daß sich — bis auf endlich viele Ausnahmen — alle Elemente aus $\mathfrak{B}$, die nicht zu $\tilde{\mathfrak{B}}$ gehören, mit Hilfe von höchstens $\left(\left[\frac{\varphi(x)}{\varphi(a)}\right] + \varphi(a) - 1\right)$ Elementen e und a aus $\tilde{\mathfrak{B}}$ darstellen lassen. Das Element a wird aber zur Darstellung von x benötigt, weil wegen (18) auch $\left(\left[\frac{\varphi(x)}{\varphi(a)}\right] + \varphi(a) - 1\right) < \varphi(x)$ ist. Nun bilden wir noch nach Satz 4 aus $\mathfrak{B}$ eine Minimalbasis $\mathfrak{B}^*$ der Ordnung $\tilde{h}$ für $\mathfrak{M}$. Diese enthält dann ebenfalls das Element a.

10. Auch die anderen Minimalbasisdefinitionen, die bei Stöhr [15] genannt werden, lassen sich verallgemeinern. Wir greifen hier nur einige Beispiele heraus und halten uns mit der Bezeichnung an [15]. Die in Nr. 8 und 9 behandelte Minimaleigenschaft entspricht den Minimalbasen 7. Art bei Stöhr.

Definition 7. *Ein Basissystem B der Ordnung h $(1 \leqq h < \infty)$ für $\mathfrak{M}$*[9]*) heißt Minimalsystem* 1. *Art, wenn für jedes Basissystem $\tilde{B}$ der Ordnung h für $\mathfrak{M}$ und alle $x \in \mathfrak{G}$ die Ungleichung $B(\| x \|) \leqq \tilde{B}(\| x \|)$ gilt.*

---

[8]) Es wird nicht ausgeschlossen, daß x mehrere solcher Darstellungen besitzt.

[9]) Hier und in den folgenden Definitionen ist natürlich immer $\mathfrak{M} \leqq \mathfrak{G}$ und $O \in \mathfrak{M}$.

Entsprechend wie für Minimalbasen 1. Art haben wir

Satz 10. *Es gibt für* $\mathfrak{M} = \mathfrak{G} = \mathfrak{Z} = \{0, 1, 2, \ldots\}$ *und* $h \geqq 2$ *keine Minimalsysteme 1. Art.*

Beweis. Das System $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ mit

$$\mathfrak{B}_1 = \{0, 1\}, \mathfrak{B}_2 = \{0, 2\}, \ldots, \mathfrak{B}_{h-1} = \{0, 2^{h-2}\}, \mathfrak{B}_h = \{0, 2^{h-1}, 2 \cdot 2^{h-1}, 3 \cdot 2^{h-1}, \ldots\}$$

ist Basissystem der Ordnung h für $\mathfrak{Z}$. Denn jede Zahl $z \in \mathfrak{Z}$ mit $t \cdot 2^{h-1} \leqq z < (t+1)\, 2^{h-1}$ $(t = 0, 1, 2, \ldots)$ ist darstellbar als $z = t \cdot 2^{h-1} + r$, wobei $0 \leqq r \leqq 2^{h-1} - 1$ ist. Also hat r eine Darstellung $r = \sum_{\eta=1}^{h-1} b^{(\eta)}$, $b^{(\eta)} \in \mathfrak{B}_\eta$.

Angenommen nun, $B_0 = \{\mathfrak{B}_1^{(0)}, \mathfrak{B}_2^{(0)}, \ldots, \mathfrak{B}_h^{(0)}\}$ wäre Minimalsystem 1. Art der Ordnung h. Dann muß wegen der Minimaleigenschaft — eventuell bei passender Umbenennung der Indizes — $\mathfrak{B}_1^{(0)}$ mit $\mathfrak{B}_1$, $\mathfrak{B}_2^{(0)}$ mit $\mathfrak{B}_2, \ldots, \mathfrak{B}_h^{(0)}$ mit $\mathfrak{B}_h$ in allen Elementen $\leqq 2^{h-1}$ übereinstimmen. Sei nun schon bewiesen, daß B_0 mit B in allen Elementen $\leqq t \cdot 2^{h-1}$ übereinstimmt $(t \geqq 1)$. Enthielte B_0 eine Zahl a mit $t 2^{h-1} < a < (t+1) 2^{h-1}$ als Element, so widerspräche das der Minimaldefinition. Andererseits muß aber wegen der Basiseigenschaft $(t+1) 2^{h-1}$ einer Menge des Systems B_0 angehören, und zwar muß $(t+1) 2^{h-1} \in \mathfrak{B}_h$ sein, da sonst nicht alle Zahlen z des Intervalls $(t+1)\, 2^{h-1} < z < (t+2)\, 2^{h-1}$ mit Hilfe von $(t+1)\, 2^{h-1}$ und Elementen aus $\mathfrak{B}_1, \ldots, \mathfrak{B}_{h-1}$ darstellbar wären. Also ist $B_0 = B$. Daraus folgt $B_0(\| n \|) = B_0(n) \geqq Cn$ $(C > 0$, const.). Jedoch konstruierte Stöhr [14] ein Basissystem B^* der Ordnung h für $\mathfrak{Z}$ mit $B^*(n) = O(\sqrt[h]{n})$, was einen Widerspruch ergibt.

Die Minimalbasisdefinitionen 2 und 3 von Stöhr [15] übertragen sich ebenfalls mühelos.

Definition 8. *Ein Basissystem* B *der Ordnung* h *für* $\mathfrak{M}$ *heißt Minimalsystem 2. Art, wenn für jedes Basissystem* $\tilde{B}$ *der Ordnung* h *für* $\mathfrak{M}$ *und alle* $x \in \mathfrak{G}$ *mit* $\| x \| \geqq \xi$ *die Ungleichung* $B(\| x \|) \leqq B(\| x \|)$ *gilt.*

Definition 9. *Ein Basissystem* B *der Ordnung* h *für* $\mathfrak{M}$ *heißt Minimalsystem 3. Art, wenn für jedes Basissystem* $\tilde{B}$ *der Ordnung* h *für* $\mathfrak{M}$ *und alle* $x \in \mathfrak{G}$ *mit* $\| x \| \geqq \xi(\tilde{B})$ *die Ungleichung* $B(\| x \|) \leqq \tilde{B}(\| x \|)$ *gilt.*

Auch hier gilt allgemein die Aussage, daß die Klasse der Minimalsysteme 3. Art (bzw. 2. Art) der Ordnung h für eine Menge $\mathfrak{M} \leq \mathfrak{G}$ höchstens abzählbar sein kann, sofern in $\mathfrak{G}$ aus $x_1 \neq x_2$ folgt $\| x_1 \| \neq \| x_2 \|$. Der Beweis verläuft ganz entsprechend wie in [6].

Als Analogon zur Stöhrschen Definition 4 haben wir

Definition 10. *Ein Basissystem* B *der Ordnung* h *für* $\mathfrak{M}$ *heißt Minimalsystem 4. Art, wenn es eine unendliche Folge* $\{x_i\}$ *von Elementen aus* $\mathfrak{G}$ *gibt, so daß für alle* x_i *und jedes Basissystem* $\tilde{B}$ *der Ordnung* h *für* $\mathfrak{M}$ *die Ungleichung* $B(\| x_i \|) \leqq \tilde{B}(\| x_i \|)$ *gilt.*

Hier können wir — im Gegensatz zu den Basen, wo die Existenz noch offen ist — zeigen

Satz 11. *Es gibt für* $\mathfrak{M} = \mathfrak{G} = \mathfrak{Z}$ *Minimalsysteme 4. Art.*

Beweis. Sei $\mathfrak{B}_\eta$ die Menge der Zahlen, die im Ziffernsystem mit der Basis 2^h die Ziffern 0 oder $2^{\eta-1}$ $(\eta = 1, 2, \ldots, h)$ haben. Dann ist, wie Stöhr [14] gezeigt hat, $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ Basissystem der Ordnung h für $\mathfrak{Z}$. Die Darstellungen der Zahlen $z \in \mathfrak{Z}$ durch das Basissystem sind auch eindeutig, da die Darstellung der Zahlen c mit

$0 \leqq c < 2^h$ im dyadischen Ziffernsystem und die Darstellung der Zahlen z im Ziffernsystem mit der Basis 2^h eindeutig ist.

Weiterhin wird bei der Darstellung der Zahlen $z_n = (2^h - 1)\sum_{\nu=0}^{n} 2^{h\nu}$ $(n = 0, 1, 2, \ldots)$ aus jeder Menge $\mathfrak{B}_\eta$ jeweils das größte Element $\leqq z_n$ benutzt, woraus folgt, daß durch das System $B^* = \{\mathfrak{B}_1^*, \ldots, \mathfrak{B}_h^*\}$, wobei $\mathfrak{B}_\eta^* = \mathfrak{B}_\eta \cap \{z \in \mathfrak{Z};\ z \leqq z_n\}$ ist, keine Zahl $z > z_n$ dargestellt wird. Damit kann kein Basissystem der Ordnung h für $\{z \in \mathfrak{Z};\ z \leqq z_n\}$ weniger Elemente als B^* enthalten, womit gezeigt ist, daß B Minimalsystem 4. Art ist.

Bemerkung: a) Durch Anwendung der Schlußweise von [6], Satz 43 läßt sich zeigen, daß die Klasse der Minimalsysteme 4. Art der Ordnung h für $\mathfrak{Z}$ von der Mächtigkeit des Kontinuums ist.

b) Definiert man: „*Ein Basissystem B der Ordnung h für $\mathfrak{M}$ heißt Minimalsystem der Art 3a, wenn für jedes Basissystem h-ter Ordnung $\tilde{B} \neq B$ für $\mathfrak{M}$ und für alle $x \in \mathfrak{G}$ mit $\| x \| \geqq \xi(\tilde{B})$ die Ungleichung $B(\| x \|) < B(\| x \|)$ gilt*“, so folgt aus Bemerkung a), daß es für keine Ordnung $h \geqq 2$ Minimalsysteme der Art 3a für $\mathfrak{Z}$ gibt, da es mindestens zwei Minimalsysteme 4. Art B_1 und B_2 mit $B_1(n_i) = B_2(n_i)$ für eine unendliche Folge $\{n_i\}$ natürlicher Zahlen gibt.

§ 4. Abschätzungen der Anzahlfunktion von Basissystemen und Basen.

11. Sei $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ ein Basissystem der Ordnung h für $\mathfrak{M}(O \in \mathfrak{M})$. Dann gilt für $h < \infty$ nach Stöhr [15], Ungleichung (49),

$$\prod_{\eta=1}^{h} (\mathfrak{B}_\eta(\xi) + 1) \geqq \mathfrak{M}(\xi) + 1, \tag{19}$$

wobei $\xi \geqq 0$ eine beliebige reelle Zahl bedeutet. Ungleichung (19) ist scharf, wie das Beispiel von Stöhr [14] zeigt.

Für eine Basis $\mathfrak{B}$ der Ordnung h für $\mathfrak{M}$ haben wir als Analogon zu dieser Ungleichung

$$\mathfrak{B}(\xi)^h + \mathfrak{B}(\xi)^{h-1} + \cdots + \mathfrak{B}(\xi) + 1 \geqq \mathfrak{M}(\xi) + 1 \quad (\xi \geqq 0 \text{ reell}). \tag{20}$$

Beweis für Ungleichung (20). Jedes der $\mathfrak{M}(\xi) + 1$ Elemente aus $\mathfrak{M}$ mit Norm $\leqq \xi$ ist darstellbar als $\sigma(b_1, \ldots, b_h)$ mit $b_\eta \in \mathfrak{B}$ und $\| b_\eta \| \leqq \xi$ $(\eta = 1, \ldots, h)$. Da $\mathfrak{B}(\xi)^\eta$ die Anzahl der Variationen η-ter Klasse von $\mathfrak{B}(\xi)$ Elementen ist, bedeutet das i-te Glied der linken Seite von Ungleichung (20) die Anzahl der höchstens möglichen (verschiedenen) Summen $\sigma(b_1, \ldots, b_{h-i+1}, O, \ldots, O)$ mit $b_1, \ldots, b_{h-i+1} \neq O$ und die ganze linke Seite die Anzahl der höchstens möglichen (verschiedenen) Summen $\sigma(b_1, \ldots, b_h)$ mit $b_\eta \in \mathfrak{B}$, $\| b_\eta \| \leqq \xi$.

Ungleichung (20) läßt sich mit Hilfe der Summenformel für die geometrische Reihe umformen zu

$$\begin{cases} \dfrac{\mathfrak{B}(\xi)^{h+1} - 1}{\mathfrak{B}(\xi) - 1} \geqq \mathfrak{M}(\xi) + 1 \text{ für } \mathfrak{B}(\xi) > 1, \\ h + 1 \geqq \mathfrak{M}(\xi) + 1 \text{ für } \mathfrak{B}(\xi) = 1. \end{cases} \tag{21}$$

Setzen wir voraus, daß die in $\mathfrak{G}$ erklärte Summe kommutativ ist, so haben wir in Analogie zu Stöhr [15] Ungleichung (1)

$$\binom{\mathfrak{B}(\xi) + h}{h} \geqq \mathfrak{M}(\xi) + 1 \tag{22}$$

für jede Basis $\mathfrak{B}$ der Ordnung h für $\mathfrak{M} \leqq \mathfrak{G}$, $0 \in \mathfrak{M}$.

Oft genügt es, wenn man an Stelle von (19) die schwächere Ungleichung

$$\sum_{\eta=1}^{h} \binom{B(\xi)}{\eta} \geqq \mathfrak{M}(\xi) \tag{23}$$

benutzt, wobei B ein Basissystem der Ordnung h für $\mathfrak{M}$ und ξ eine reelle Zahl $\geqq 0$ bedeutet.

Beweis von (23). Die Binomialkoeffizienten liefern jeweils die Anzahl der Kombinationen η-ter Klasse ohne Wiederholung ($\eta = 1, \ldots, h$), und daher umfaßt das i-te Glied in (23) alle Darstellungen der Form $\sigma(b_1, \ldots, b_h)$ ($b_\eta \in \mathfrak{B}_\eta$), wobei $h - i$ Elemente b_η gleich O sind.

Für den Fall, daß $\mathfrak{G}$ kommutativ und assoziativ ist und

$$\| \sigma(x, y) \| = \| x \| + \| y \| \quad (x, y \in \mathfrak{G})$$

gilt, haben wir als Verschärfung von (22)

$$\mathfrak{M}(\xi) \leqq \sum_{\substack{b_i \in \mathfrak{B} \\ 0 < \|b_i\| \leqq \xi}} \binom{\mathfrak{B}(\xi - \| b_i \|) + h - 1}{h - 1}.$$

Beweis. Jedes $y \in \mathfrak{M} \cap \{x \in \mathfrak{G};\ 0 < \| x \| \leqq \xi\}$ ist darstellbar als $\sigma(b_1, \ldots, b_h)$, $b_\eta \in \mathfrak{B}$. Für jedes feste $b_i \in \{b_1, \ldots, b_h\}$ muß dann unter Benutzung der obigen Voraussetzungen $\| \sigma(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_h) \| \leqq \xi - \| b_i \|$ gelten. Das heißt, es kommen bei festem $b_i \neq 0$ insgesamt

$$\binom{\mathfrak{B}(\xi - \| b_i \|) + h - 1}{h - 1}$$

verschiedene Summen $\sigma(b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_h)$ zur Darstellung in Betracht. Demnach folgt

$$\mathfrak{M}(\xi) \leqq \sum_{\substack{b_i \in \mathfrak{B} \\ 0 < \|b_i\| \leqq \xi}} \binom{\mathfrak{B}(\xi - \| b_i \|) + h - 1}{h - 1}.$$

Für $h = 2$ erhalten wir entsprechend wie in [7]

$$\mathfrak{M}(\xi) \leqq \sum_{\substack{b_i \in \mathfrak{B} \\ \|b_i\| \leqq \xi}} \mathfrak{B}(\xi - \| b_i \|).$$

12. Entsprechend wie bei Basen für die Menge der nichtnegativen ganzen Zahlen definieren wir, wenn $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ ein Basissystem der Ordnung h ($h < \infty$) für die Menge $\mathfrak{M} \leqq \mathfrak{G}$ ist,

$$\beta_1^* = \underline{\operatorname{fin}}_{\substack{x \in \mathfrak{G} \\ x \neq O}} \frac{B(\| x \|)}{\sqrt[h]{\mathfrak{M}(\| x \|)}}, \quad \beta_2^* = \underline{\lim}_{\substack{x \in \mathfrak{G} \\ x \neq O}} \frac{B(\| x \|)}{\sqrt[h]{\mathfrak{M}(\| x \|)}}, \quad \beta_3^* = \overline{\lim}_{\substack{x \in \mathfrak{G} \\ x \neq O}} \frac{B(\| x)\|}{\sqrt[h]{\mathfrak{M}(\| x \|)}},$$

$$\beta_4^* = \overline{\operatorname{fin}}_{\substack{x \in \mathfrak{G} \\ x \neq O}} \frac{B(\| x \|)}{\sqrt[h]{\mathfrak{M}(\| x \|)}}$$

und $\nu_i^*(h) = \underline{\operatorname{fin}}_{B}\, \beta_i^*$ ($i = 1, 2, 3, 4$), wobei bei der Bildung des $\underline{\operatorname{fin}}_{B}$ von B alle Basissysteme der Ordnung h für $\mathfrak{M}$ durchlaufen werden.

Für Basen $\mathfrak{B}$ der Ordnung h für $\mathfrak{M}$ haben wir entsprechend die Quotienten $\dfrac{\mathfrak{B}(\| x \|)}{\sqrt[h]{\mathfrak{M}(\| x \|)}}$ zu betrachten, die analogen Größen β_i zu bilden und $\nu_i(h) = \underline{\operatorname{fin}}_{\mathfrak{B}}\, \beta_i$ ($i = 1, 2, 3, 4$) zu

setzen. Dabei gilt

Satz 12. $\frac{\nu_i^*(h)}{h} \leqq \nu_i(h) \leqq \nu_i^*(h)$ $(i = 1, 2, 3, 4)$.

Beweis. Sei $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ ein Basissystem der Ordnung h für $\mathfrak{M}$. Durch $\mathfrak{B} = \bigcup_{\eta=1}^{h} \mathfrak{B}_\eta$ erhalten wir eine Basis der Ordnung h für $\mathfrak{M}$. Dann gilt nach Nr. 6

$$\frac{B(\xi)}{h} \leqq \mathfrak{B}(\xi) \leqq B(\xi) \text{ für alle } \xi \geqq 0,$$

also

$$\frac{1}{h}\,\frac{B(\|x\|)}{\sqrt[h]{\mathfrak{M}(\|x\|)}} \leqq \frac{\mathfrak{B}(\|x\|)}{\sqrt[h]{\mathfrak{M}(\|x\|)}} \leqq \frac{B(\|x\|)}{\sqrt[h]{\mathfrak{M}(\|x\|)}} \text{ für alle } x \in \mathfrak{G}, \quad x \neq O,$$

und somit

$$\frac{1}{h}\,\beta_i^* \leqq \beta_i \leqq \beta_i^* \text{ für jedes Basissystem der Ordnung } h \text{ für } \mathfrak{M},$$

$$\frac{1}{h}\,\nu_i^*(h) \leqq \nu_i(h) \leqq \nu_i^*(h) \qquad (i = 1, 2, 3, 4).$$

Weiterhin ist selbstverständlich $\nu_i^*(h) \leqq \nu_{i+1}^*(h)$ bzw. $\nu_i(h) \leqq \nu_{i+1}(h)$ $(i = 1, 2, 3)$.

Die Größen $\nu_i^*(h)$ und $\nu_i(h)$ stehen auf folgende Weise mit Minimalsystemen und Minimalbasen in Zusammenhang:

Satz 13. *Ist B Minimalsystem* 1. *Art der Ordnung h für $\mathfrak{M}$, so ist hierfür $\beta_1^* = \nu_1^*(h)$ und $\beta_4^* = \nu_4^*(h)$.*

Beweis. Angenommen, es wäre $\beta_1^* > \nu_1^*(h)$, dann gäbe es ein Basissystem B_0 der Ordnung h für $\mathfrak{M}$ und ein Element $x_0 \in \mathfrak{G}$ mit

$$\frac{B_0(\|x_0\|)}{\sqrt[h]{\mathfrak{M}(\|x_0\|)}} < \frac{B(\|x_0\|)}{\sqrt[h]{\mathfrak{M}(\|x_0\|)}},$$

also

$$B_0(\|x_0\|) < B(\|x_0\|),$$

was einen Widerspruch bedeutet.

Für den zweiten Teil der Behauptung verläuft der Beweis entsprechend.

Satz 14. *Ist B Minimalsystem* 2. *oder* 3. *Art der Ordnung h für $\mathfrak{M}$, so ist hierfür $\beta_2^* = \nu_2^*(h)$ und $\beta_3^* = \nu_3^*(h)$.*

Beweis. Angenommen, es wäre $\beta_2^* > \nu_2^*(h)$, dann gäbe es ein Basissystem B_0 der Ordnung h für $\mathfrak{M}$ und eine unendliche Folge $\{x_i\}$ von Elementen aus $\mathfrak{G}$, so daß

$$\frac{B_0(\|x_i\|)}{\sqrt[h]{\mathfrak{M}(\|x_i\|)}} < \frac{B(\|x_i\|)}{\sqrt[h]{\mathfrak{M}(\|x_i\|)}}$$

ist, also

$$B_0(\|x_i\|) < B(\|x_i\|),$$

was einen Widerspruch bedeutet.

Der zweite Teil der Behauptung läßt sich analog beweisen.

Bemerkung: Für Basen gelten entsprechende Aussagen.

Es ist eine wichtige Aufgabe, diese Größen $\nu_i^*(h)$ und $\nu_i(h)$ zu bestimmen bzw. abzuschätzen. Wir betrachten dabei zuerst

13. *Basissysteme.* Für $\nu_1^*(h)$ zeigen wir

Satz 15. *Es ist* $\nu_1^*(h) \geqq 1$ *unabhängig von der Menge* $\mathfrak{M} \leqq \mathfrak{G}$.

Beweis. Sei B ein Basissystem der Ordnung h für $\mathfrak{M}$. Wegen

$$1 \leqq \frac{B(\|x\|)}{h} < \frac{B(\|x\|)}{h-1} < \cdots < \frac{B(\|x\|)}{2} \quad \text{für} \quad B(\|x\|) \geqq h$$

folgt

$$\binom{B(\|x\|)}{\eta} \leqq \frac{B(\|x\|)^\eta}{\eta!} \leqq \frac{B(\|x\|)^h}{h!} \qquad (\eta = 1, \ldots, h).$$

Somit erhalten wir aus (23)

$$h\,\frac{B(\|x\|)^h}{h!} \geqq \mathfrak{M}(\|x\|) \text{ für alle } x \in \mathfrak{G} \text{ mit } \|x\| \geqq N,$$

wobei $N = N(B)$ so bestimmt ist, daß für alle x mit $\|x\| \geqq N$ gilt $B(\|x\|) \geqq h$. Daraus folgt

$$\frac{B(\|x\|)^h}{\mathfrak{M}(\|x\|)} \geqq (h-1)!,$$

$$\operatorname*{fin}_{x \in \mathfrak{G},\, \|x\| \geqq N} \frac{B(\|x\|)}{\sqrt[h]{\mathfrak{M}(\|x\|)}} \geqq \sqrt[h]{(h-1)!} \geqq 1.$$

Wäre nun $\nu_1^*(h) < 1$, dann gäbe es nach dem Vorangehenden ein Basissystem h-ter Ordnung B_0 für $\mathfrak{M}$ und ein $x_0 \in \mathfrak{G}$ mit $\|x_0\| < N(B_0)$, so daß $\dfrac{B_0(\|x_0\|)}{\sqrt[h]{\mathfrak{M}(\|x_0\|)}} < 1$ wird. Dann wären mit $B_0(\|x_0\|) = t \leqq h-1$ Elementen und O mehr als t^h Elemente aus $\mathfrak{M}$ darstellbar. Also wäre unter Benutzung von (23)

$$\sum_{\eta=1}^{h} \binom{t}{\eta} > t^h.$$

Die Summe auf der linken Seite ist aber gleich $2^t - 1$, also wäre $2^t - 1 > t^h$, woraus wegen $t \leqq h-1$ folgt $2^{h-1} > t^h$, was für $t > 1$ einen Widerspruch bedeutet. Den Widerspruch für $t = 1$ erkennt man direkt aus $2^1 - 1 > 1^h$. Also muß gelten $\nu_1^*(h) \geqq 1$.

Betrachten wir für die Menge $\mathfrak{G}$ speziell die Menge $\mathfrak{Z}$ der nichtnegativen ganzen Zahlen und nehmen wir auch $\mathfrak{M} = \mathfrak{G} = \mathfrak{Z}$, so erhalten wir durch $B = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_h\}$ mit $\mathfrak{B}_1 = \{0, 1\}$, $\mathfrak{B}_2 = \cdots = \mathfrak{B}_h = \{0, 2, 3, \ldots\}$ ein Basissystem der Ordnung h für $\mathfrak{Z}$. Für dieses Basissystem wird

$$\operatorname*{fin}_{\substack{x \in \mathfrak{Z} \\ x \neq O}} \frac{B(\|x\|)}{\sqrt[h]{\mathfrak{Z}(\|x\|)}} = \operatorname*{fin}_{\substack{x \in \mathfrak{Z} \\ x \neq O}} \frac{B(x)}{\sqrt[h]{x}} \leqq \frac{B(1)}{\sqrt[h]{1}} = 1.$$

Demnach gilt für diesen Spezialfall $\nu_1^*(h) = 1$.

Für $\nu_2^*(h)$ läßt sich als Abschätzung angeben:

Satz 16. $\nu_2^*(h) \geqq h$.

Beweis. Damit $\beta_2^* = \lim\limits_{\substack{x \in \mathfrak{G} \\ x \neq O}} \dfrac{B(\|x\|)}{\sqrt[h]{\mathfrak{M}(\|x\|)}} = \lim\limits_{\substack{x \in \mathfrak{G} \\ x \neq O}} \dfrac{\sum\limits_{\eta=1}^{h} \mathfrak{B}_\eta(\|x\|)}{\sqrt[h]{\mathfrak{M}(\|x\|)}}$ minimal ausfällt, müssen die Zähler der Brüche, also $\sum\limits_{\eta=1}^{h} \mathfrak{B}_\eta(\|x\|)$ möglichst klein sein. In Verbindung mit Un-

gleichung (19) folgt hieraus $\mathfrak{B}_\eta(\| x \|) + 1 \geqq \sqrt[h]{\mathfrak{M}(\| x \|) + 1}$ $(\eta = 1, \ldots, h)$. Denn besteht für h positive Größen $y_1, \ldots, y_h$ die Forderung $\prod_{\eta=1}^{h} y_\eta \geqq C$, so ist $\sum_{\eta=1}^{h} y_\eta$ minimal für $y_1 = \cdots = y_h$. Demnach erhalten wir

$$\beta_2^* \geqq \varliminf_{\substack{x \in \mathfrak{G} \\ x \neq 0}} \frac{h \sqrt[h]{\mathfrak{M}(\| x \|) + 1} - h}{\sqrt[h]{\mathfrak{M}(\| x \|)}} = h,$$

das heißt $\nu_2^*(h) \geqq h$.

Nehmen wir als wichtiges Beispiel wieder den Sonderfall $\mathfrak{G} = \mathfrak{M} = \mathfrak{Z}$; Stöhr [14] konstruierte ein Basissystem h-ter Ordnung für $\mathfrak{Z}$, für das er $\nu_2^*(h) = h$ zeigte (Stöhr [15], Ungleichung (19)). Also haben wir in diesem Fall $\nu_2^*(h) = h$.

14. *Basen in nicht notwendig kommutativen Mengen* $\mathfrak{G}$. Wir untersuchen nun die Größen $\nu_i(h)$ und zeigen zunächst:

Satz 17. *Es ist* $\nu_1(h) \geqq \dfrac{1}{\sqrt[h]{h}}$ *unabhängig von der Menge* $\mathfrak{M} \leqq \mathfrak{G}$.

Beweis. Da die linke Seite von Ungleichung (20) durch $h\mathfrak{B}(\| x \|)^h + 1$ vergrößert wird, folgt

$$h\mathfrak{B}(\| x \|)^h \geqq \mathfrak{M}(\| x \|),$$

$$\mathfrak{B}(\| x \|) \geqq \frac{\sqrt[h]{\mathfrak{M}(\| x \|)}}{\sqrt[h]{h}},$$

$$\beta_1 \geqq \frac{1}{\sqrt[h]{h}}$$

und

$$\nu_1(h) \geqq \frac{1}{\sqrt[h]{h}}.$$

Für $\mathfrak{G} = \mathfrak{M} = \mathfrak{Z}$ gibt Stöhr [15] ein Beispiel einer Basis h-ter Ordnung mit $\beta_1 = \dfrac{1}{\sqrt[h]{h}}$.

Eine Abschätzung für $\nu_2(h)$ gibt

Satz 18. $\nu_2(h) \geqq 1$.

Der *Beweis* folgt sofort aus Satz 12.

15. *Basen in kommutativen Mengen* $\mathfrak{G}$. Um in diesem Fall die Größen $\nu_i(h)$ zu untersuchen, gehen wir von Abschätzung (22) aus. Entsprechend wie bei Stöhr [15] zeigt man

Satz 19. $\nu_1(h) \geqq \dfrac{1}{\sqrt[h]{h}}$

und

Satz 20. $\nu_2(h) \geqq \sqrt[h]{h!}$.

§ 5. Vielfachheit von Darstellungen.

16. Sind $\mathfrak{A}$ und $\mathfrak{B}$ Mengen nichtnegativer ganzer Zahlen, so haben oft Elemente von $\mathfrak{A} + \mathfrak{B}$ mehrere Darstellungen der Form $a + b$, $a \in \mathfrak{A}$, $b \in \mathfrak{B}$. Aussagen über sich hieraus ergebende Fragen stammen von G. G. Lorentz [8], G. A. Dirac [3] und Erdös-Turan [5].

Wir wollen hier nun allgemeiner den Fall betrachten, daß $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ Untermengen einer Menge $\mathfrak{G}$ sind, in der die in Nr. 2 definierte Summe $\sigma(a_1, \ldots, a_n)$ für alle n-Tupel $\{a_1, \ldots, a_n\}$ mit $a_\nu \in \mathfrak{A}_\nu$ $(\nu = 1, \ldots, n)$ von ω verschieden ist. Kommutativität und Assoziativität wird nicht vorausgesetzt. Jedoch soll für diesen Paragraphen für einen festen Index i $(1 \leqq i \leqq n)$ aus

$$\sigma(a_1, \ldots, a_{i-1}, a_i, a_{i+1}, \ldots, a_n) = \sigma(a_1, \ldots, a_{i-1}, a_i', a_{i+1}, \ldots, a_n)$$

folgen $a_i = a_i'$ für alle Kombinationen von Elementen $a_\nu, a_\nu' \in \mathfrak{A}_\nu$ $(\nu = 1, \ldots, n)$. Über die Norm setzen wir außerdem noch statt (15) die Dreiecksungleichung

$$\| \sigma(a_1, \ldots, a_n) \| \leqq \sum_{\nu=1}^{n} \| a_\nu \| \qquad (a_\nu \in \mathfrak{A}_\nu)$$

sowie

$$\varliminf_{\substack{x \in \mathfrak{G} \\ x \neq 0}} \frac{\mathfrak{G}(\varkappa \| x \|)}{\mathfrak{G}(\| x \|)} \to 1 \text{ für } \varkappa \to 1.$$

voraus.

Gilt $\sigma(a_1, \ldots, a_n) = \sigma(a_1', \ldots, a_n') = c$ $(a_\nu, a_\nu' \in \mathfrak{A}_\nu;\ \nu = 1, \ldots, n)$, dann sollen diese Darstellungen für c dann und nur dann identisch heißen, wenn $a_\nu = a_\nu'$ ist $(\nu = 1, \ldots, n)$. Mit $\varrho(x)$, $x \in \mathfrak{G}$, bezeichnen wir die Anzahl der verschiedenen Darstellungen von x als $x = \sigma(a_1, \ldots, a_n)$ $(a_\nu \in \mathfrak{A}_\nu,\ a_\nu \neq 0;\ \nu = 1, \ldots, n)$. Dann ist $\varrho(x)$ für jedes $x \in \mathfrak{G}$ als nichtnegative ganze Zahl definiert. Wir beweisen damit folgende Sätze:

Satz 21. *Sei $\alpha_\nu = \underline{D}(\mathfrak{A}_\nu)$ die asymptotische Dichte der Menge $\mathfrak{A}_\nu$ $(\nu = 1, \ldots, n)$. Ist $\alpha_i > 0$ und ist mindestens ein $\mathfrak{A}_\nu (\nu \neq i)$ eine unendliche Menge, dann gibt es eine Menge $\mathfrak{M} \leqq \sum_{\nu=1}^{n} \mathfrak{A}_\nu \leqq \mathfrak{G}$ mit $\underline{D}(\mathfrak{M}) \geqq \alpha_i$ und $\lim_{x \in \mathfrak{M}} \varrho(x) = \infty$. (Dabei hat der Index i die Bedeutung, wie sie oben eingeführt wurde.)*

Beweis. Seien $\varepsilon_\nu < 1$ beliebige positive reelle Zahlen $(\nu = 1, \ldots, n)$ mit $\sum_{\nu=1}^{n} \varepsilon_\nu = 1$ und $\mathfrak{C} \leqq \mathfrak{G}$ eine beliebige Menge. Ferner sei $x \in \mathfrak{G}$ zunächst ein festes Element. Mit N bezeichnen wir die Summe der Anzahlen der (verschiedenen) Darstellungen aller Elemente $y \in \mathfrak{G}$ mit $0 < \| y \| \leqq \| x \|$ als $y = \sigma(a_1, \ldots, a_n)$, wobei $a_\nu \in \mathfrak{A}_\nu$ den Bedingungen $0 < \| a_\nu \| \leqq \varepsilon_\nu \| x \|$, $\nu = 1, \ldots, n$, genügen soll. Dann gilt unter Benutzung der Dreiecksungleichung offenbar

$$N = \prod_{\nu=1}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|). \tag{24}$$

Andererseits überschreitet die Anzahl der Darstellungen von $y \in \mathfrak{G}$, $0 < \| y \| \leqq \| x \|$, mit obiger Zusatzbedingung weder $\varrho(y)$ noch $\prod_{\substack{\nu=1 \\ \nu \neq i}}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|)$ wegen der Zusatzvoraussetzung über die Summe. Also haben wir auch

$$N \leqq \sum_{\substack{y \in \mathfrak{G} \\ 0 < \|y\| \leqq \|x\| \\ y \notin \mathfrak{C}}} \varrho(y) + \mathfrak{C}(\| x \|) \prod_{\substack{\nu=1 \\ \nu \neq i}}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|). \tag{25}$$

Durch Vergleich von (24) und (25) erhalten wir

$$\prod_{\nu=1}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|) \leqq \sum_{\substack{y \in \mathfrak{G} \\ 0 < \|y\| \leqq \|x\| \\ y \notin \mathfrak{C}}} \varrho(y) + \mathfrak{C}(\| x \|) \prod_{\substack{\nu=1 \\ \nu \neq i}}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|)$$

und

$$\frac{\mathfrak{C}(\| x \|)}{\mathfrak{G}(\| x \|)} \geqq \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)}{\mathfrak{G}(\| x \|)} - \sum_{\substack{y \in \mathfrak{G} \\ 0 < \|y\| \leqq \|x\| \\ y \notin \mathfrak{C}}} \varrho(y) \frac{\left(\prod\limits_{\substack{\nu=1 \\ \nu \neq i}}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|)\right)^{-1}}{\mathfrak{G}(\| x \|)}, \tag{26}$$

wo wir nur die $x \in \mathfrak{G}$ betrachten, für die $\mathfrak{A}_\nu(\varepsilon_\nu \| x \|) > 0$ ist ($\nu = 1, \ldots, n;\ \nu \neq i$).

Sei r eine natürliche Zahl und $\mathfrak{C}_r$ die Menge der Elemente aus $\mathfrak{G}$, die mindestens r Darstellungen der Form $\sigma(a_1, \ldots, a_n)$ ($a_\nu \in \mathfrak{A}_\nu$, $a_\nu \neq 0$) zulassen. Ist $y \notin \mathfrak{C}_r$, dann haben wir $\varrho(y) < r$ und daher auf Grund von (26)

$$\frac{\mathfrak{C}_r(\| x \|)}{\mathfrak{G}(\| x \|)} \geqq \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)}{\mathfrak{G}(\| x \|)} - r\left(\prod_{\substack{\nu=1 \\ \nu \neq i}}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|)\right)^{-1}.$$

für jedes ε_i mit $0 < \varepsilon_i < 1$,

$$\varliminf_{\substack{x \in \mathfrak{G} \\ x \neq 0}} \frac{\mathfrak{C}_r(\| x \|)}{\mathfrak{G}(\| x \|)} \geqq \varliminf_{\substack{x \in \mathfrak{G} \\ x \neq 0}} \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)}{\mathfrak{G}(\| x \|)} = \varliminf_{\substack{x \in \mathfrak{G} \\ x \neq 0}} \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)\, \mathfrak{G}(\varepsilon_i \| x \|)}{\mathfrak{G}(\varepsilon_i \| x \|)\, \mathfrak{G}(\| x \|)} \geqq \alpha_i(1 - \delta),$$

wobei $\delta \to 0$ geht für $\varepsilon_i \to 1$. Daher folgt $\underline{D}(\mathfrak{C}_r) \geqq \alpha_i$. Für jedes r können wir nun ein N_r so groß bestimmen, daß

$$\frac{\mathfrak{C}_r(\| x \|)}{\mathfrak{G}(\| x \|)} \geqq \alpha_i - 2^r$$

ist für alle x mit $\| x \| \geqq N_r$. Weiter können wir annehmen, daß die Zahlen N_r für $r \to \infty$ nicht beschränkt bleiben. Sei $\mathfrak{M}$ die Menge der Elemente aus $\mathfrak{G}$, für die

$$\mathfrak{M} \cap \{y \in \mathfrak{G};\ N_r \leqq \| y \| < N_{r+1}\} = \mathfrak{C}_r \cap \{y \in \mathfrak{G};\ N_r \leqq \| y \| < N_{r+1}\} \quad (r = 1, 2, \ldots)$$

ist. Dann gilt für $x \in \mathfrak{M}$, $N_r \leqq \| x \| < N_{r+1}$,

$$\frac{\mathfrak{M}(\| x \|)}{\mathfrak{G}(\| x \|)} \geqq \frac{\mathfrak{C}_r(\| x \|)}{\mathfrak{G}(\| x \|)} \geqq \alpha_i - 2^r.$$

Folglich wird

$$\varliminf_{\substack{x \in \mathfrak{G} \\ x \neq 0}} \frac{\mathfrak{M}(\| x \|)}{\mathfrak{G}(\| x \|)} \geqq \alpha_i$$

und $\lim\limits_{x \in \mathfrak{M}} \varrho(x) = \infty$, womit Satz 21 bewiesen ist.

Bemerkung: Für $\alpha_\nu = 0$ ($\nu = 1, \ldots, n$) braucht keine Menge $\mathfrak{M}$ mit den angegebenen Eigenschaften zu existieren, wie Beispiele sofort zeigen.

Satz 22. *Seien $\mathfrak{A}_\nu \subseteq \mathfrak{G}$ mit $\underline{D}(\mathfrak{A}_\nu) = \alpha_\nu > 0$ ($\nu = 1, \ldots, n$). Außerdem möge in $\mathfrak{G}$ gelten $\mathfrak{G}(\xi) \geqq C\xi$ für alle genügend großen ξ mit einer positiven Konstanten C sowie $\varliminf\limits_{\substack{x \in \mathfrak{G} \\ x \neq 0}} \frac{\mathfrak{G}(\varkappa \| x \|)}{\mathfrak{G}(\| x \|)} = \varkappa$ ($0 < \varkappa < 1$)*[10]*. Dann gibt es*

[10]) Allgemein existiert $\lim\limits_{\substack{x \in \mathfrak{G} \\ x \neq 0}} \frac{\mathfrak{G}(\varkappa\xi)}{\mathfrak{G}(\xi)}$ nicht.

a) *im Fall* $n > 2$ *zu jedem* $\delta > 0$ *eine Menge* $\mathfrak{M}$ *mit der asymptotischen Dichte* $\underline{D}(\mathfrak{M}) = \mu \geqq \alpha_i \, (i = 1, \ldots, n)$,

b) *im Fall* $n = 2$ *zu jedem* δ *mit* $0 < \delta < \dfrac{C^2}{(C+1)^2} \alpha_1 \alpha_2$ *eine Menge* $\mathfrak{M}$ *mit*

$$\underline{D}(\mathfrak{M}) = \mu \geqq \alpha_1 \left(1 - \frac{C+1}{C} \sqrt{\frac{\delta}{\alpha_1 \alpha_2}}\right) > 0,$$

so daß $\varrho(x) \geqq \delta \, \| x \|$ *für alle* $x \in \mathfrak{M}$ *ist.*

Beweis. Sei $0 < \varepsilon'_\nu < \alpha_\nu$ $(\nu = 1, \ldots, n;\ \nu \neq i)$ und es bedeute $\mathfrak{M}$ die Menge der Elemente $x \in \mathfrak{G}$, für die $\varrho(x) \geqq \delta \, \| x \|$ ist. Auf Grund von Ungleichung (26) folgt

$$\begin{aligned}
\frac{\mathfrak{M}(\| x \|)}{\mathfrak{G}(\| x \|)} &\geqq \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)}{\mathfrak{G}(\| x \|)} - \frac{\left(\prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|)\right)^{-1}}{\mathfrak{G}(\| x \|)} \delta \sum_{\substack{y \in \mathfrak{M}\\ 0 < \|y\| \leqq \|x\|}} \| y \| \\
&\geqq \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)}{\mathfrak{G}(\| x \|)} - \frac{\left(\prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|)\right)^{-1}}{\mathfrak{G}(\| x \|)} \delta \sum_{\substack{y \in \mathfrak{G}\\ 0 < \|y\| \leqq \|x\|}} \| y \| \\
&\geqq \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)}{\mathfrak{G}(\| x \|)} - \frac{\left(\prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} \mathfrak{A}_\nu(\varepsilon_\nu \| x \|)\right)^{-1}}{\mathfrak{G}(\| x \|)} \delta \| x \| \, \mathfrak{G}(\| x \|) \\
&\geqq \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)}{\mathfrak{G}(\| x \|)} - \frac{\delta \| x \|}{\prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} \{(\alpha_\nu - \varepsilon'_\nu) \, \mathfrak{G}(\varepsilon_\nu \| x \|)\}}
\end{aligned}$$

für alle $x \in \mathfrak{G}$ mit genügend großer Norm. Weiter haben wir

$$\varliminf_{\substack{x \in \mathfrak{G}\\ \|x\| \geqq N}} \frac{\mathfrak{M}(\| x \|)}{\mathfrak{G}(\| x \|)} \geqq \varliminf_{\substack{x \in \mathfrak{G}\\ \|x\| \geqq N}} \frac{\mathfrak{A}_i(\varepsilon_i \| x \|)}{\mathfrak{G}(\varepsilon_i \| x \|)} \frac{\mathfrak{G}(\varepsilon_i \| x \|)}{\mathfrak{G}(\| x \|)} - \varlimsup_{\substack{x \in \mathfrak{G}\\ \|x\| \geqq N}} \frac{\delta \| x \|}{\left(\prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} (\alpha_\nu - \varepsilon'_\nu)\right) C^{n-1} \| x \|^{n-1} \prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} \varepsilon_\nu},$$

wobei für $\| x \| \to \infty$ auch $\varepsilon'_\nu \to 0$ geht $(\nu = 1, \ldots, n;\ \nu \neq i)$. Also folgt

$$\begin{aligned}
\mu &\geqq \alpha_i \varepsilon_i - \varlimsup_{\substack{x \in \mathfrak{G}\\ \|x\| \geqq N}} \frac{\delta}{\prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} (\alpha_\nu - \varepsilon'_\nu) \, C^{n-1} \| x \|^{n-2} \prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} \varepsilon_\nu} \quad \text{für } n > 2 \text{ mit } \prod_{\substack{\nu=1\\ \nu \neq i}}^{n} \varepsilon_\nu \geqq k > 0, \\
&\geqq \alpha_1 \varepsilon_1 - \frac{\delta}{\alpha_2 C \varepsilon_2} \quad \text{für } n = 2, \quad i = 1.
\end{aligned}$$

Im Fall $n > 2$ lassen wir $\varepsilon_i \to 1$ gehen, jedoch mit der Nebenbedingung $\| x \|^{n-2} \prod\limits_{\substack{\nu=1\\ \nu \neq i}}^{n} \varepsilon_\nu \to \infty$. Dann erhalten wir $\mu \geqq \alpha_i$.

Für $n = 2$, $i = 1$ haben wir $\varepsilon_1 = 1 - \varepsilon_2$, und wir wählen $\varepsilon_2 = \sqrt{\frac{\delta}{\alpha_1 \alpha_2}}$, woraus folgt

$$\mu \geqq \alpha_1(1 - \varepsilon_2) - \frac{\delta}{\alpha_2 C \sqrt{\frac{\delta}{\alpha_1 \alpha_2}}} \geqq \alpha_1 \left(1 - \sqrt{\frac{\delta}{\alpha_1 \alpha_2}} - \frac{1}{C} \sqrt{\frac{\delta}{\alpha_1 \alpha_2}}\right)$$

$$\geqq \alpha_1 \left(1 - \frac{C+1}{C} \sqrt{\frac{\delta}{\alpha_1 \alpha_2}}\right).$$

Bemerkung: Die Aussage bleibt natürlich bestehen, wenn im Fall $n = 2$ die Mengen $\mathfrak{A}_1$ und $\mathfrak{A}_2$ ihre Rollen vertauschen.

§ 6. Spezialfälle.

17. Die bisher in der Literatur behandelten Basisbegriffe lassen sich durch geeignete Spezialisierungen aus dem hier allgemein definierten Basisbegriff herleiten.

(a)

Setzt man $\mathfrak{G} = \mathfrak{Z} = \{0, 1, 2, \ldots\}$ und an Stelle der Funktion $\sigma(a_1, \ldots, a_n)$ die gewöhnliche Addition, also $\sigma(a_1, \ldots, a_n) = \sum_{\nu=1}^{n} a_\nu$ $(a_\nu \in \mathfrak{Z})$, so erhält man den Basisbegriff, wie er von Schnirelmann [13] eingeführt und von Rohrbach [12], Stöhr [15] u. a. untersucht wurde. Dabei ist als Norm der Elemente der Betrag zu nehmen. — Wird hierbei für $\mathfrak{G}$ eine endliche Untermenge $\{0, 1, 2, \ldots, n\}$ von $\mathfrak{Z}$ genommen, so erhält man Abschnittsbasen.

(b)

Wird die Komposition in $\mathfrak{G}$ erklärt durch

$$\sigma(a_1, \ldots, a_n) = \begin{cases} \sum_{\nu=1}^{n} a_\nu & \text{für } a_\alpha \neq a_\beta \quad (1 \leqq \alpha < \beta \leqq n) \\ \omega & \text{sonst,} \end{cases}$$

so folgt der Begriff der 1-Basis (Härtter [6]).

(c)

Bedeutet $\mathfrak{Z}^*$ die Menge aller ganzen rationalen Zahlen, dann liefert $\mathfrak{G} = \mathfrak{Z}^*$ und

$$\sigma(a_1, a_2) = a_1 - a_2,$$
$$\sigma(a_1, \ldots, a_n) = \omega \text{ für } n > 2$$

Differenzbasen (Rédei-Rényi [11] und Erdös-Gál [4]). Jedoch genügt der Betrag als Norm einer Zahl dann nicht Bedingung (15). Sätze, die diese Forderung beim Beweis nicht benutzen (wie z. B. Satz 4), gelten auch hier.

(d)

Sei $\mathfrak{G} = \mathfrak{Z}^*$ und $\sigma(a_1, \ldots, a_n) = \sum_{\nu=1}^{n} a_\nu$ $(1 \leqq n < \infty)$. De Bruijn [1] nennt eine Menge $\mathfrak{A} < \mathfrak{G}$ Basis, wenn jedes $x \in \mathfrak{G}$ *eindeutig* als $x = \sigma(a_1, \ldots, a_n)$ $(a_\nu \in \mathfrak{A};\ a_\alpha \neq a_\beta$ für $\alpha \neq \beta)$ darstellbar ist.

(e)

Mit $\mathfrak{G} = \{1, 2, 3, \ldots\}$ und $\sigma(a_1, \ldots, a_n) = \prod_{\nu=1}^{n} a_\nu$ folgt der Begriff der Produktbasis, wie er von Raikov [10] eingeführt wurde.

(f)

Nimmt man für $\mathfrak{G}$ die Menge $\mathfrak{Z}_r$ der r-dimensionalen Vektoren mit nicht-negativen ganzzahligen Komponenten und wird die Summe durch die Addition der Vektoren erklärt, so erhält man Basen für Gitterpunktmengen ([7]). Die Beträge der Vektoren lassen sich dann als Norm verwenden. Die in [7] benutzte Anzahlfunktion ist jedoch speziell für Mengen von Vektoren eingerichtet und nutzt mehr deren Anordnung aus als die hier allgemein definierte Anzahlfunktion.

Eine interessante Verallgemeinerung ergibt sich hieraus, wenn man als Menge $\mathfrak{G}$ nur die Vektoren aus $\mathfrak{Z}_r$ betrachtet, die in einem mit der Spitze im Nullpunkt liegenden Kegel enthalten sind.

(g)

Sei $\mathfrak{G} = \mathfrak{R}$ die Menge der nichtnegativen rationalen Zahlen. Als Komposition in $\mathfrak{G}$ nehmen wir die gewöhnliche Addition und die Norm definieren wir auf folgende Weise:

1.) $\| 0 \| = 0$,

2.) Sei $x \in \mathfrak{R}$, $x \neq 0$ und $x = \frac{\alpha}{\beta}$ die Normalform der Bruchdarstellung von x, also α und β natürliche Zahlen und $(\alpha, \beta) = 1$. Dann setzen wir $\| x \| = \max(\alpha, \beta)$. Die so erklärte Norm genügt den Bedingungen (12) bis (14), wie man sich sofort überzeugt. An Stelle obiger Norm kann man auch nehmen $\| O \| = 0$, $\| x \| = \left\| \frac{\alpha}{\beta} \right\| = \alpha + \beta$ für $x \neq O$. Der Betrag der rationalen Zahlen als Norm erfüllt aber nicht die Forderung (12), und auch eine p-adische Bewertung für $\mathfrak{R}$ genügt nicht den Bedingungen (12) bis (15).

(h)

Steinhaus [16] untersucht Basen für Mengen von reellen Zahlen. Hierzu ist $\mathfrak{G}$ gleich einer geeigneten Menge von reellen Zahlen zu setzen, während als Komposition Summe oder Differenz zu nehmen ist. Allerdings sind hier nicht alle Bedingungen (12) bis (15) für den Betrag als Norm erfüllt, so daß nicht alle hier allgemein bewiesenen Sätze angewandt werden können.

(i)

Sei $\mathfrak{G}$ ein Verband, in dem wir aber nur die Verknüpfung $\cup$ betrachten. Hierdurch erhalten wir in $\mathfrak{G}$ eine Komposition, die die Forderungen an die Summe in Nr. 2 erfüllt. Das Element O wird durch die leere Menge dargestellt. Durch die Beziehung $\leqq$ läßt sich in $\mathfrak{G}$ eine Teilordnung einführen, die den Forderungen (12) bis (15) genügt, sofern die Gesamtheit aller oberen Nachbarn jedes Elements aus $\mathfrak{G}$ endlich ist. Dabei hat die leere Menge die Norm 0, alle oberen Nachbarn davon die Norm 1 usw. Hat allgemein ein Element $x \in \mathfrak{G}$ die Norm $\| x \| = n$, dann haben alle oberen Nachbarn von x die Norm $n + 1$. Die Gültigkeit der Dreiecksungleichung ist aber nicht in jedem Fall gewährleistet.

18. Hat man in $\mathfrak{G}$ mehrere Kompositionen, die alle der Definition in Nr. 2 genügen und die Forderungen (12) bis (15) erfüllen, so lassen sich unsere Betrachtungen auch auf diesen Fall anwenden. Sei $\mathfrak{S} = \{\sigma, \tau, \ldots\}$ eine Menge von Operatoren, die auf die

Elemente $\mathfrak{a} \in \Gamma$ angewandt entweder ein Element $c \in \mathfrak{G}$ oder ω ergeben, dann gelten für jedes Element aus $\mathfrak{S}$ die Sätze über Basen.

Hier ordnet sich der Begriff der erweiterten Basis (Rohrbach [12]) ein, indem man $\mathfrak{G} = \mathfrak{Z}$ nimmt und für die Operatoren $\sigma, \tau, \ldots$ die Kombinationen von $h - \alpha$ Zeichen $+$ und α Zeichen $-$ setzt $(0 \leqq \alpha \leqq h - 1)$. Jedoch ist bei der Anwendung der Sätze zu beachten, daß für dieses Beispiel Forderung (15) nicht gilt.

Literatur.

[1] *N. G. de Bruijn*, On bases for the set of integers. Publ. math., Debrecen **1** (1949/50), 232—242.

[2] *J. G. van der Corput-J. H. B. Kemperman*, The second pearl of the theory of numbers. I, II, III. Akad. Wetensch., Proc. **52** (1949), 696—704, 801—809, 927—937 = Indagationes Math. **11** (1949), 226—234, 277—285, 325—335.

[3] *G. A. Dirac*, Note on a problem in additive number theory. Journ. London Math. Soc. **26** (1951), 312—313.

[4] *P. Erdös-J. S. Gál*, On the representation of $1, 2, \ldots, N$ by differences. Proc. Acad. Wet., Amsterdam **51** (1948), 1155—1158 = Indagationes math. **10** (1948), 379—382.

[5] *P. Erdös-P. Turan*, On a problem of Sidon in additive number theory and on some related problems. Journ. London Math. Soc. **16** (1941), 212—215.

[6] *E. Härtter*, Ein Beitrag zur Theorie der Minimalbasen. Journ. reine angew. Math. **196** (1956), 170—204.

[7] *E. Härtter*, Basen für Gitterpunktmengen. Journ. reine angew. Math. **202** (1959), 153—170.

[8] *G. G. Lorentz*, Multiplicity of representations of integers by sums of elements of two given sets. Journ. London Math. Soc. **28** (1953), 464—467.

[9] *D. Raikov*, Über die Basen der natürlichen Zahlenreihe. Mat. Sbornik N. S. **2** (= **44**) (1937), 595—597.

[10] *D. Raikov*, On multiplicative bases for the natural series. Mat. Sbornik N. S. **3** (= **45**) (1938), 569—576.

[11] *L. Rédei-A. Rényi*, Über die Darstellung der Zahlen $1, 2, \ldots, N$ mittels Differenzen. Mat. Sbornik N. S. **24** (= **66**) (1949), 385—389.

[12] *H. Rohrbach*, Ein Beitrag zur additiven Zahlentheorie. Math. Zeitschr. **42** (1937), 1—30.

[13] *L. Schnirelmann*, Über additive Eigenschaften von Zahlen. Math. Ann. **107** (1933), 649—690.

[14] *A. Stöhr*, Eine Basis h-ter Ordnung für die Menge aller natürlichen Zahlen. Math. Zeitschr. **42** (1937), 739—743.

[15] *A. Stöhr*, Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. Journ. reine angew. Math. **194** (1955), 40—65, 111—140.

[16] *H. Steinhaus*, Eine neue Eigenschaft der Menge von G. Cantor. Wektor, Warszawa **7** (1917).

[17] *B. Volkmann*. Bemerkung über Gitterbasen. Journ. reine angew. Math. **202** (1959), 171—173.

Eingegangen 15. März 1960.

für

an
+
zu

kad.
234,

313.
n 51

urn.

204.

ndon

576.
S. 24

743.
Math.